

JP3949679

Publication Title:

STEGANOGRAPHIC SYSTEM

Abstract:

Abstract of JP 2005051793

(A) PROBLEM TO BE SOLVED: To improve a steganographic system and applications therefor, more particularly to facilitate scale and rotation registration for steganographic decoding, to decode without accessing originals which are not coded, to increase robustness of steganographic coding and/or in the presence of lossy compression/decompression, and to make energy in a spatial domain facilitate decoding registration in motion pictures.

Courtesy of <http://v3.espacenet.com>

(18) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-51793

(P2005-51793A)

(43) 公開日 平成17年2月24日(2005.2.24)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04N 1/387	H04N 1/387	5B057
G06T 1/00	G06T 1/00 500B	5C076

審査請求 有 請求項の数 46 O L (全 115 頁)

(21) 出願番号	特願2004-224727 (P2004-224727)	(71) 出願人	500111792
(22) 出願日	平成16年7月30日(2004.7.30)		ディジマール コーポレーション
(82) 分類の表示	特許第38-334238の分類		アメリカ合衆国 オレゴン州 97008
	第1出願日 平成8年5月7日(1996.5.7)		、 ビーヴァートン、 エスタブリッシュ ジェミニ ドライヴ 9405
(31) 優先権主張番号	08/436,102	(74) 代理人	100094318
(32) 優先日	平成7年5月8日(1995.5.8)		弁理士 山田 行一
(33) 優先権主張国	米国(US)		
(31) 優先権主張番号	08/508,083	(72) 発明者	ローズ ジェフリー ビー
(32) 優先日	平成7年7月27日(1995.7.27)		アメリカ合衆国 オレゴン州 97068
(33) 優先権主張国	米国(US)		ウェスト リン エスタブリッシュ トッ
(31) 優先権主張番号	08/512,993		アラウン ループ 304
(32) 優先日	平成7年8月9日(1995.8.9)	ドターム(参考)	5B057 AA20 CA12 CA16 CB12 CB16
(33) 優先権主張国	米国(US)		CB19 CB08 CH20 DA20 DB02
(31) 優先権主張番号	08/534,005		5C076 AA14 BA06
(32) 優先日	平成7年9月25日(1995.9.25)		
(33) 優先権主張国	米国(US)		

最終頁に続く

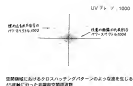
(54) 【発明の名称】 ステガノグラフィシステム

(57) 【要約】 (修正有)

【課題】ステガノグラフィシステムおよびその用途の改善であり、具体的にはステガノグラフィの復号化に関するスケールおよび回転整合を容易にすること、符号化されていないオリジナルにアクセスすることなく復号化すること、動画におけるおよび/または損失的圧縮/伸張のステガノグラフィの符号化の堅牢性を増すことと、空間領域におけるエネルギーが復号化整合を容易にすることである。

【解決手段】回転対称にステガノグラフィ的に埋め込まれたパターン、およびサブピクセルディジタルグラフィキュールを使用し、パターン化ビットセルによってデータを表す。用途は、拡張セキュリティ金庫取引と、偽造防止識別カードと、セルラ電話用詐欺防止システムと、ビデオ送信における隠れモデムチャネルと、自動著作権検出を有する写真複製キオスクと、インターネットにおいて使用する。例えば、URLを埋め込まれたホットリンク化画像オブジェクトを含む。

【図1】図29



【特許請求の範囲】

【請求項1】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法であって、前記方法は、

画像画像を含むデジタル画像を受信する工程と、

前記デジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、

識別コードを表す2次元のコード信号を生成する工程であって、前記2次元コード信号は、デジタル画像での位置に対応している要素を有し、且つ前記位置上で識別コードがランダム化されて繰り返し分布されるよう生成される、前記生成工程と、

2次元コード信号に基づいてデジタル画像を変更することによって、識別コードをデジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーションを可能にする、前記生成工程と、

を含む方法。

【請求項2】

前記識別コードはURLアドレスを備える、請求項1に記載の方法。

【請求項3】

前記識別コードは、ネットワーク資源を見つけるのに用いられるインデックスを備える、

請求項1に記載の方法。

【請求項4】

前記識別コードは、前記2次元コード信号のブロックで繰り返される、請求項1に記載の方法。

【請求項5】

前記オブジェクトに登録データをステガノグラフィ的に埋め込み、前記オブジェクトの印刷バージョンから画像を走査することによって生じる凹陥およびスケール変更を補正する、請求項1に記載の方法。

【請求項6】

前記登録データは、周波数領域でパターンを備える、請求項5に記載の方法。

【請求項7】

前記登録データは、前記2次元コード信号によって形成されるパターンを備える、請求項5に記載の方法。

【請求項8】

前記2次元コード信号は、デジタル画像の対応する画像に応じて変化して、前記オブジェクトでの識別コードの知覚可能性を低減する、請求項1に記載の方法。

【請求項9】

前記2次元コード信号は、前記デジタル画像から独立している鍵に属している、請求項1に記載の方法。

【請求項10】

前記鍵は、データオブジェクトで識別コードをランダム化するために用いられる、請求項1に記載の方法。

【請求項11】

前記識別コードは、オブジェクトをネットワーク上のデータベースに関連付けているインデックス情報を含む、請求項1に記載の方法。

【請求項12】

前記デジタル画像はカラー画像を備え、前記ステガノグラフィック埋め込みは前記カラー画像の輝度を変更することによって実行される、請求項1に記載の方法。

【請求項13】

前記識別コードは2以上のビットを含み、前記2次元コード信号は、前記オブジェクトの複数の画素のそれぞれが2ビット以上の情報によって変更されるように、前記デジタル画像を変更する。請求項1に記載の方法。

【請求項14】

前記2次元コード信号の要素は前記デジタル画像の画素ブロックに対応し、前記要素は、前記画素ブロックの特徴を変調して前記識別コードを埋め込む。請求項1に記載の方法。

【請求項15】

前記要素は、低周波数に前記識別コードの信号エネルギーが集中するように前記画素ブロックの特徴を変調する。請求項14に記載の方法。

【請求項16】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法であって、前記方法は、

前記オブジェクトの画像を走査して、前記オブジェクトを表す画素要素を含むデジタル画像を形成する工程と、

前記デジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記デジタル画像にステガノグラフィ的に埋め込まれた2次元のコード信号で運ばれ、前記2次元コード信号は、デジタル画像内の位置に対応している要素を有し、前記2次元コード信号は、前記位置上で前記識別コードをランダム化して、繰り返し分布している。前記工程と、

前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトから前記ネットワーク資源へのナビゲーションを可能にしている。前記工程と、

を含む方法。

【請求項17】

前記デジタル画像の特徴を解析して前記識別コードのビットを抽出する工程を含む。請求項16に記載の方法。

【請求項18】

前記デジタル画像の統計的特徴を解析して前記識別コードのビットを抽出する工程を含む。請求項17に記載の方法。

【請求項19】

前記デジタル画像の画素ブロックの特徴を解析して前記識別コードのビットを抽出する工程を含む。請求項17に記載の方法。

【請求項20】

異なる極性が前記識別コードのビットの異なるビット値を伝達するのに用いられる。請求項16に記載の方法。

【請求項21】

前記デジタル画像の画素のそれぞれが前記識別コードの2以上のビットを伝達する。請求項16に記載の方法。

【請求項22】

前記識別コードはURLアドレスを備える。請求項16に記載の方法。

【請求項23】

前記識別コードは、ネットワーク資源を見つけるのに用いられるインデックスを備える。請求項16に記載の方法。

【請求項24】

前記識別コードは、前記2次元コード信号のブロックで繰り返される。請求項16に記載の方法。

【請求項25】

前記デジタル画像から登録データをステガノグラフィ的に復号化し、前記オブジェクト

の旧バージョンから画像を走査することによって生じる回転およびスケール変更を修正する。請求項16に記載の方法。

【請求項25】

前記登録データは、周波数領域でパターンを備える。請求項25に記載の方法。

【請求項26】

前記登録データは、前記2次元コード信号によって形成されるパターンを備える。請求項25に記載の方法。

【請求項28】

前記2次元コード信号は、前記デジタル画像から独立している鍵に従属している。請求項16に記載の方法。

【請求項29】

前記鍵は、前記デジタル画像から前記識別コードのビットを復号するのに用いられる。請求項28に記載の方法。

【請求項30】

前記鍵がランダム特性を有する。請求項29に記載の方法。

【請求項31】

前記識別コードは、オブジェクトをネットワーク上のデータベースに関連づけているインデックス情報を含む。請求項16に記載の方法。

【請求項32】

前記デジタル画像はカラー画像を備え、前記ステガノグラフィ的復号化は前記カラー画像の輝度から前記識別コードのビットを抽出することによって実行される。請求項16に記載の方法。

【請求項33】

幾何登録は、前記画像をステガノグラフィ的に埋め込まれた登録パターンに相関させることによって実行される。請求項16に記載の方法。

【請求項34】

相関を実行して、前記デジタル画像から前記識別コードのビットを抽出する工程を含む。請求項16に記載の方法。

【請求項35】

エラー訂正コーディングを用いて、前記デジタル画像から前記識別コードのビットを抽出する工程を含む。請求項16に記載の方法。

【請求項36】

信頼性の重み付けを用いて、前記識別コードのビット値を抽出する際にエラーを低減する工程を含む。請求項35に記載の方法。

【請求項37】

オブジェクトから、ネットワークに記憶された前記オブジェクト関連の情報へのナビゲーションを管理するシステムであって、前記システムは、

オブジェクトにステガノグラフィ的に埋め込まれた識別コードの登録所であって、前記識別コードおよび前記ステガノグラフィックコードが埋め込まれた前記オブジェクト関連情報を記憶している、前記登録所と、

前記オブジェクトからステガノグラフィ的に復号化される識別コードを受信するサーバであって、前記識別コードを用いて前記オブジェクト関連情報を得るのに使用可能な、前記サーバと、
を備えるシステム。

【請求項38】

前記サーバおよび登録所は、インターネットからアクセスでき、前記オブジェクトから復号化された前記識別コードに応じてオブジェクト関連情報を提供する。請求項37に記載のシステム。

【請求項39】

前記識別コードはURLアドレスを備える。請求項37に記載のシステム。

【請求項40】

前記識別コードがデータベースへのインデックスを備え、前記データベースは、前記インデックスに対応するアドレス情報を記憶し、前記アドレス情報は、前記オブジェクトに関連したネットワーク資源をナビゲートするのに用いられる、請求項37に記載のシステム

【請求項41】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法を実行する命令を格納する記憶媒体であって、前記方法が、

画像画像を含むデジタル画像を受信する工程と、

前記デジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、

前記識別コードを表す2次元のコード信号を生成する工程であって、前記2次元コード信号はデジタル画像での位置に対応している要素を有していて、且つ前記位置上で識別コードがランダム化されて繰り返し分布されるよう生成される、前記生成工程と、

2次元コード信号に基づいてデジタル画像を変更することによって、識別コードをデジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーションを可能にする、前記生成工程と、

を含む、記憶媒体。

【請求項42】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法を実行する命令を格納する記憶媒体であって、

前記方法が、

前記オブジェクトの画像を走査して、前記オブジェクトを表す画像画像を含むデジタル画像を形成する工程と、

前記デジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記デジタル画像にステガノグラフィ的に埋め込まれた2次元のコード信号で覆われ、前記2次元コード信号は、デジタル画像内の位置に対応している要素を有していて、且つ前記位置上で前記識別コードをランダム化して、繰り返し分布している、前記工程と、

前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトからネットワーク資源へのナビゲーションを可能にしている、前記工程と、

を含む、記憶媒体。

【請求項43】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法であって、前記方法が、

画像画像を含むデジタル画像を受信する工程と、

前記デジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、

識別コードを表す2次元のコード信号を生成する工程であって、前記2次元コード信号はデジタル画像での位置に対応している要素を有していて、且つ前記位置上で識別コードが繰り返し分布されるよう生成される、前記生成工程と、

2次元コード信号に基づいてデジタル画像を変更することによって、識別コードをデジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーション

を可能にする、前記生成工程と、を含む方法。

【請求項4】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるようオブジェクトに情報を埋め込む方法であって、前記方法は、

画像要素を含むデジタル画像を受信する工程と、

前記デジタル画像に埋め込まれる識別コードを受信する工程であって、前記コードがネットワーク資源の位置決めをするのに用いられる、前記受信工程と、

識別コードを表す2次元のコード信号を生成する工程であって、前記2次元コード信号はデジタル画像での位置に対応している要素を有していて、且つ前記位置上で識別コードがランダム化されて分布されるよう生成される、前記生成工程と、

2次元コード信号に基づいてデジタル画像を変更することによって、識別コードをデジタル画像にステガノグラフィ的に埋め込み、ネットワーク資源にリンクしたオブジェクトを生成する工程であって、前記識別コードは、オブジェクトの印刷バージョンから走査された画像から機械で読み取り可能であり、ネットワーク資源へのナビゲーションを可能にする、前記生成工程と、を含む方法。

【請求項5】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法であって、前記方法は、

前記オブジェクトの画像を走査して、前記オブジェクトを表す画像要素を備えているデジタル画像を形成する工程と、

前記デジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記デジタル画像にステガノグラフィ的に埋め込まれた2次元のコード信号で覆われ、前記2次元コード信号は、デジタル画像内の位置に対応している要素を有していて、且つ前記位置上で前記識別コードをランダム化している、前記工程と、

前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトからネットワーク資源へのナビゲーションを可能にしている、前記工程と、を含む方法。

【請求項6】

オブジェクトからネットワーク資源へのネットワークナビゲーションが可能になるよう、オブジェクトからステガノグラフィ的に埋め込まれた情報を復号化する方法であって、前記方法は、

前記オブジェクトの画像を走査して、前記オブジェクトを表す画像要素を備えているデジタル画像を形成する工程と、

前記デジタル画像から識別コードをステガノグラフィ的に復号化する工程であって、前記識別コードは、前記デジタル画像にステガノグラフィ的に埋め込まれた2次元のコード信号で覆われ、前記2次元コード信号は、デジタル画像内の位置に対応している要素を有していて、且つ前記位置上で前記識別コードを繰り返し分布している、前記工程と、

前記識別コードを用いて、ネットワーク上でネットワーク資源を位置決めする工程であって、前記識別コードは、前記オブジェクトからネットワーク資源へのナビゲーションを可能にしている、前記工程と、を含む方法。

【発明の詳細な説明】

【ステガノグラフィの背景】

【0001】

ステガノグラフィに対する多数のアプローチと、ステガノグラフィの多数の用途とが存

とする。概略は以下の通りである。

【0002】

ゾーン イー エム アイに対する米国特許公開明細書第2196167号は、オーディオ記録を記録のオーナを示すマーキング信号と電子的に混合し、その組み合わせがオリジナルと加算的に同一であるシステムを開示している。米国特許明細書第4963998号および第5079648号は、このシステムの変形例を開示している。

【0003】

ボルト、ペレナックおよびニューマンに対する米国特許明細書第5319735号は、前述のゾーン イー エム アイの特許と同じ原理に基礎を置いているが、精神音響マスキング問題を追加で述べている。

【0004】

モーゼスに対する米国特許明細書第4425642号、第4425661号、第5404377号および第5473631号は、データをオーディオ信号にごくわずかに埋め込む種々のシステムを開示しており、後者の2つの特許は、特に、ニューラルネットワーク実現化と、組郡の知覚的符号化とに焦点を置いている。

【0005】

エー ティー アント ティーに対する米国特許明細書第4943973号は、低レベルノイズ信号を他のデータに追加し、これらと共に補助データを伝送する拡張スペクトル技術を用いるシステムを開示している。この特許は、ネットワーク制御信号をデジタル化音声信号と共に送信する状況において特に説明している。

【0006】

ユー エス フィリップスに対する米国特許明細書第5161210号は、追加の低レベル量子化レベルを、オーディオ信号において規定し、これらと共に、例えば、コピー禁止信号を伝送するシステムを開示している。

【0007】

クロスに対する米国特許明細書第4972471号は、著作権が取得された素材に関するオーディオ（例えば、ラジオ）信号の、これらに隣接下に埋め込まれた識別信号の参照による自動的な監視において援助することを目的とするシステムを開示している。

【0008】

デジーンに対する米国特許明細書第5243423号は、ランダムに選択されたビデオラインにおいてデジタルデータ（例えば、番組企業識別、著作権マーキング、媒体調査、非公開説明、等のデータ）を符号化するヒドステガノグラフィシステムを開示している。デジーンは、テレビジョン同期パルスに頼り、デジタルデータによってXORされ、ビデオと結合された格納された疑似ランダムシーケンスをトリガする。

【0009】

欧州特許出願公開明細書第5181317号は、画像を多ビット識別コードと共に冗長的にマーキングするシステムを開示している。前記コードの各々の“1”（“0”）ビットを、複数の間隔を置いて離れた“署名点”の間隔の真素値におけるわずかな増加（減少）として明らかにする。疑わしい画像とオリジナルの非符号化画像との差を計算し、前記署名点の間隔の両側変動を検査することによって復号化を進める。

【0010】

PCT明細書WO95/14289号は、この分野における本明細書に先行する仕事である。

【0011】

コマンダは、彼らの論文“文書画像通信における電子透かしにおける提案と、署名を実現化するためのその用途”、日本における電子および通信、パート1、73巻、No. 5、1990年、22〜33ページにおいて、画像マーキング技術を説明している。この仕事は、理解することがいくらか困難であるが、透かし（例えば、1ビット符号化メッセージ）が疑わしい画像において存在するかどうかの単純なイエス／ノー決定に明らかに帰着する。

【0012】

ビデオ信号へのデジタル情報の埋め込みに関する多数の仕事が存在する。多くは、垂直および水平帰線消去期間のような信号の非視覚的部分への埋め込みを行うが、他のものは、この情報を“パンドラ”（すなわち、可視ビデオ信号それ自身）に埋め込む。例は、米国特許明細書第4,528,588号、第4,595,950号および第5,319,453号と、欧州特許出願公開明細書第4,417,022号と、マツビル、”ビデオステガノグラフィ：署名を画像に秘密に埋め込む方法”、アイ・エム・ユー・加納財産プロジェクト会報、1994年1月、1巻、第1版、187～205ページとを含む。

【0013】

ビデオおよびマルチメディアの著作権マーキングにおいて、ヨーロッパにおいて種々のコンソーシアムの研究の試みが存在する。技術の概説は、“画像のアクセス制御および著作権保護（ACCOPI）”、ワークパッケージ8：透かし、1995年6月30日、46ページにおいて見られる。タリスマンと呼ばれる新たな計画は、このACCOPI仕事をある程度拡張すると思われる。これらの計画において活動的な研究者オおよびコーは、シスコ社として知られるウェブを基礎とする電子媒体マーキングサービスを提供している。

【0014】

オーフは、彼の論文“不可視通信”、ヘルシンキ技術大学、デジタルシステム研究室、1995年11月5日において、ステガノグラフィの多数の問題を調査している。

【0015】

スタンフォード2世他は、“データ埋め込み方法”、SPIE 2615巻、1995年10月23日において、彼らの1994年5月の動作である、画像ステガノグラフィプログラム（BMPMBED）を報告している。

【0016】

英国の企業、ハイワーク エフビーアイリミテッドは、識別情報を写真および他のグラフィカルデータにごくわずかに埋め込むソフトウェア製品を紹介している。この技術は、欧州特許明細書第9,400,971、9（1994年1月19日出願）、第9,504,221、2号（1995年3月2日出願）および第9,513,790、7号（1995年7月3日出願）とに属し、これらの最初のものは、PCT国際公開パンフレットWO95/20291号として公開されている。

【0017】

エムアイティのウォルター ベンダーは、彼の論文、“データハイディングに関する技術”、マサチューセッツ工科大学、メディア研究室、1995年1月による説明のようには、この分野における種々の仕事を行っている。

【0018】

パロアルトのダイス社は、エージェントの名の下で示されるオーディオマーキング技術を開発している。米国特許が未決定であることが理解され、まだ発行されていない。

【0019】

ティケル他は、モナッシュ大学において、例えば、“電子すかしマーク”、BITA-93、マッカリー大学、シドニー、オーストラリア、1993年12月と、“電子すかし”IEEE 画像における国際会議、1994年11月13～16日、86～90ページとを含む種々の論文を発表している。

【0020】

NRECテクニカルリサーチインスティテュートのコックス他は、“マルチメディアの保護拡張スベクトルすかし”と表題の付いた1995年12月の彼らの論文において、種々のデータ埋め込み技術を考察している。

【0021】

モレー他は、“Technergestutzte Steganographie: Wie sie funktioniert und warum es falsch ist, jede Reglementierung von Verschlüsselung unsinnig ist. Daß Datensicherheit und Datensicherung, 18/6(1994) 318-326 において、ISDNにおいて補助データを命令

的に埋め込む実験的なシステムを考案している。このシステムは、I S D N信号標本を取り上げ、変更し、しきい値以下の標本信号に関する補助データ送信を引き上げる。

【0022】

一般的に、隔すべきメッセージストリームからのビットを直接またはオーディオ信号の最下位ビットと交換することによって動作する。インターネット（例えば、“ステコ”および“ホワイトノイズストーム”において利用可能な種々のソフトウェアプログラムが存在する。

【0023】

詳細な説明

説明的な実施例の以下の論考において、言葉“信号”および“画値”を、1、2および2を越える偶数の次元のデジタル信号に言及するに交換可能に使用する。例を、1次元オーディオ形式デジタル信号と2次元画像形式デジタル信号との間で前後に順列的に切り換える。

【0024】

本発明の説明的な実施例の詳細を十分に説明するために、最初にデジタル信号の基本的な性質を説明することが必要である。図1は、1次元デジタル信号の古典的な表現を示す。x軸は、デジタルの配列“標本”のインデックス番号を規定し、y軸は、デジタル標本の“2進深度”として規定される有限数のレベルのみにおける存在に即断されている標本における信号の瞬間的な値である。図1に示す図は、標本値の16の許可された状態を与える4乗または“4ビット”に対して2の値を有する。

【0025】

音波のようなオーディオ情報に関して、デジタル化処理は、連続した現象を時間領域および信号レベル領域の双方において離散的に取り扱うと、一般的に認識されている。そのようなものとして、デジタル化の処理それ自身が、基本的なエラー原因をもたらし、いずれかの領域における離散的な処理期間より小さい細部を記録することができない。産業界はこれを、時間領域において“エイリアシング”と呼び、信号レベル領域において“量子化ノイズ”と呼ぶ。このように、デジタル信号の基本エラーフロアが、常に存在する。実効的意味において測定された純粋な量子化ノイズは、12の平方根を1越えた値か、0、29 d B程度の値を有することが理論的に既知であり、ここでD Nは、“デジタル数”または信号レベルの最も細かい単位増分を表す。例えば、完全な12ビットデジタルタイザは、 ~ 0 、29 d Bの固有実効ノイズフロアを作り、4096の許可されたD Nを有する。

【0026】

すべての既知の物理測定定理は、連続信号のデジタル形式への交換に追加のノイズを加える。代表的に量子化ノイズは、後に言及するように、直角位相（二乗平均の平方根）において、測定処理の“アナログノイズ”に加わる。

【0027】

ほとんどすべての商業的および技術的処理によるデシベルスケールの使用は、所定の記録媒体における信号およびノイズの測定として使用される。“信号ノイズ比”という表現は、一般に、本明細書におけるように使用される。例として、本明細書は、信号ノイズ比を、信号パワーおよびノイズパワーの項として言及し、したがって20 d Bは、信号振幅における10倍の増加を表す。

【0028】

要約において、本発明の現在の好適な実施例は、全体の信号に、純粋なノイズの形状を有する非常に小さい振幅の符号化信号の付加によってNビット値を埋め込んだ。通常Nを、少なくとも8とし、Nビット値の復旧および復号化における数論的な信号ノイズの考慮によって、より高い精度にする。実効的な問題として、Nを、所望の固有の真実な“署名”の数のような、用途の特定に基づいて選択する。説明するために、N=128とすると、固有のデジタル署名の数は、 10^{-38} （ 2^{-128} ）以上になる。この数は、十分な統計的な確実性をもって作品を検証することと、情報の正確な復元および

び配布を示すことの双方に対して十分な値以上であると思われる。

【0029】

この追加の信号の振幅またはパワーは、この方法論を使用する各々すべての用途の、審美的および情報の考慮によって決定する。例えば、非聴覚的なビデオは、平均的な人間の眼に目立つことなく、より高い埋め込み信号レベルを有することができる。高精度オーディオは、“ヒス”における不連続な増加を人間の耳が加減しないように比較的小さい信号レベルのみを使用することができる。これらの方法は、一般的なものであり、各々の用途は、埋め込み信号の信号レベルの選択において、それ自身の基準の組を有する。埋め込み信号のより高いレベルは、より悪質なコピーを検証することができる。他方では、埋め込み信号のより高いレベルは、より不快な増大されるノイズが、もしかすると配布される作品の価値に影響を及ぼすかもしれない。

【0030】

本発明の原理を用いることができる異なった用途の範囲を説明するために、本明細書は、2つの異なるシステムを詳述する。第1のもの（よりよい名前が無いために、“ハッシュ符号化”システムと呼ぶ）は、存在するデータ信号に検証符号化を用いる。第2のもの（よりよい名前が無いために、“リアルタイム符号化”と呼ぶ）は、発生された信号に検証符号化を用いる。これらの当業者は、本発明の原理を、特に記述したこれらに加えて、多くの他の状況に用いることができることを認識するであろう。

【0031】

これらの2つのシステムの論考を、どちらの順番で読むこともできる。何人かの読み手は、後者が前者より直観的であることに気づき、他の者にとっては、その反対が真実であろう。

【0032】

ハッシュ符号化

実施例の第1の組の以下の論考は、関連する用語を規定する段階によって最も良く始められる。

【0033】

オリジナル信号を、オリジナルデジタル信号か、非デジタル信号の高品質にデジタル化されたコピーに適用する。

【0034】

Nビット検証ワードを、8から128までのNレンジを代表的に有し、開示された変換処理を経て最終的にオリジナル信号において配置される検証コードである、固有検証2進値に適用する。示された実施例において、各々のNビット検証ワードは、値“0101”の配列から始まり、残りの信号（後述する定義を参照）における信号ノイズ比の最適化を決定するのに使用される。

【0035】

Nビット検証ワードのm番目のビット値を、Nビットワードの左から右に読んだときのm番目の位置に値に対応するゼロまたは1のいずれかとする。例えば、N=8検証ワード01110100の第1（m=1）ビット値は、値“0”であり、この検証ワードの第2ビット値は、“1”である。等。

【0036】

m番目の独立埋め込みコード信号を、オリジナル信号に正確に等しい次元および量（例えば、双方が12か48の512デジタル画像）を有し、（示した実施例においては）デジタル値の独立した擬似ランダムな配列である信号に適用する。“擬似”は、純粋なランダム状態を哲学的に決定する困難に敬意を払い、“ランダム”信号を発生する種々の許容しうる方法が存在することを示す。いかなる所定のオリジナル信号にも、関連する正確にN個の独立した埋め込みコード信号が存在する。

【0037】

許容しうる増大されるノイズレベルを、どの位の“余分のノイズ”、すなわち次に記述する複合埋め込みコード信号の振幅を、オリジナル信号に追加し、脱売または別な方法の

配布に対して許容しうる信号を依然として有しているかの用途固有の決定に適用する。本明細書は、許容しうる代表的な値としてノイズにおける1 dBの増加を使用するが、これは、全く任意である。

【0038】

複合理の込みコード信号は、オリジナル信号と正確に等しい次元および量（例えば、双方が5 12かける5 12デジタル画像）を有し、Nの複合理の込みコード信号の追加で固有の減衰を含む信号に適用する。独立埋め込みコードを、任意のスケールにおいて発生するが、複合信号の振幅は、前もってセットされた許容しうる知覚されるノイズレベルを越えてはならず、したがってNの追加独立コード信号の“減衰”を必要とする。

【0039】

配布可能信号を、オリジナル信号に複合理の込みコード信号を加えたものから成る、オリジナル信号とはほぼ同様のコピーに適用する。これは、外部の社会に配布され、オリジナル信号より僅かに高い許容しうる“ノイズ特性”を有する信号である。

【0040】

疑わしい信号を、オリジナルおよび配布された信号の全体的な外観を有し、そのオリジナルに検証が一致する可能性を疑われている信号に適用する。疑わしい信号がNビット検証ワードに一致する場合、解析すれば分かる。

【0041】

この第1実施例の詳細な方法論は、Nビットワードをmビット値の各々にこれらの対応する結果として複合信号中に蓄積される独立埋め込みコード信号を乗算することによってオリジナル信号に埋め込むことから始まり、完全に合計された複合信号を次に許容しうる知覚されるノイズ振幅に減衰させ、結果として得られるオリジナル信号に加えられた複合信号が配布可能信号になる。

【0042】

次にオリジナル信号とNビット検証ワードとすべてのNの独立埋め込みコード信号とを、安全な場所に格納する。次に疑わしい信号を見つける。この信号は、多数のコピー、圧縮および伸長、異なった間隔のデジタル信号への再標本化、デジタルからアナログへそこから戻ってデジタル媒体への変換、またはこれらの項目のなんらかの組み合わせを受けたかもしれない。この信号が、依然としてオリジナルと同様に見える場合、すなわちその本質的な性質が、これらの変換およびノイズの付加のすべてによってまったく破壊されない場合、埋め込み信号のノイズ特性に対する信号に応じて、検証処理を、統計上の確実さのある目的の程度に機能させるべきである。疑わしい信号の改ざんの程度と、オリジナルの許容しうる知覚されるノイズレベルとを、検証の要求される信頼性レベルの2つのキーパラメータとする。

【0043】

疑わしい信号における検証処理を、疑わしい信号をデジタルフォーマットおよびオリジナル信号の範囲に再標本化および整理することによって始める。したがって画像が2の因子によって減少している場合、同じ因子によってデジタル的に増大させる必要がある。さらに、音楽の一部が“削除”されているが依然としてオリジナルと同一標本化率を有する場合、オリジナルのこの削除部分を記録する必要があり、これを代表的に、2つの信号の局所デジタル相関（通常のデジタル操作）を行い、これの見つけた差延値を使用して、オリジナルの部分に対するこの断部分を記録することによって行う。

【0044】

疑わしい信号をオリジナルに対して標本化間隔を一致させ記録すると、疑わしい信号の信号レベルを実際の意味においてオリジナルの信号レベルに一致させるべきである。これを、オフセット、2つの信号間のエラーの二乗平均の最小値を前記増幅及びゲインのパラメータの関数として使用することによって最適化されている前記3つのパラメータを探索することによって行うことができる。この点において規格化され記録された、または便利のために単に規格化された疑わしい信号を呼び出すことができる。

【0045】

このとき新たに適合された対は、規格化された疑わしい信号から減算されたオリジナル信号を有し、差信号を提供する。次に差信号を、N種の独立なランダムコード信号と記録されたピーク相関値の各々と相互に相関させる。第1の4ビットコード（“0101”）を、0値および1値の平均値と、ノイズ値がより上層の信号を望むなら2つの信号の異なる整合との双方におけるキャリアフレークとして使用する（すなわち、0101の最適な分値は、2つの信号の最適な整合を示し、Nビット検証信号の確然的な存在が存在することも示す）。

【0046】

結果として得られるピーク相関値は、0101キャリアレーション配列によって見つけれられた0および1の平均値に近接することにより0および1に変換することができる浮動小数点数のノイズの組を形成する。疑わしい信号が本当にオリジナルから得られたものである場合、上述した処理から結果として得られる検証数は、オリジナルのNビット検証ワードと一致し、“ビットエラー”統計が予測されたものか既知でないものかを示す。信号-ノイズの考慮は、検証処理においてある種類の“ビットエラー”が存在する場合、検証のX%の確率の状態で働くことを決定し、ここでXは、99.9%であることが望まれる。疑わしい信号が本当にオリジナルのコピーではない場合、0および1の本質的にランダムな配列が発生し、結果として生じる値の分離の明らかな不足が発生する。すなわち、結果として得られる値をヒストグラムにプロットすると、Nビット検証信号の存在は強い2レベル特性を示すが、コードの非存在または異なるオリジナルの異なるコードの存在は、ランダムな正規分布形式の形式を示す。このヒストグラムの分離は、検証に対して十分であるが、正確なバイナリ配列を客観的に再生できる場合、検証のより強い証拠となる。

【0047】

特別な例

カクテルパーティーにおける二人の国家首座の高価な絵を手に入れ、この絵が市場においてある妥当な報酬を得るに値するものが確実であるとする。我々は、この絵を売ることを望み、許可されないまたは支払われない方法で使われていないことを保証する、このことと以下のステップとを、図2において要約する。

【0048】

この絵を、陽画のカラープリントに変換すると仮定する。我々は始めにこれを、代表的な光度測定スペクトル応答曲線を有する通常の高品質白黒スキャナによって、デジタル化された形式に走査する（カラー画像の3原色の各々において走査することによって、ノイズ比に対してより良い最終的な信号を得ることができ、このニュアンスは、基本的な処理を記述することに対しては重要ではない）。

【0049】

ここで、走査された画像は、12ビットグレイ値または4096の許可されたレベルによって規定される精度のグレイスケールを有する4000×4000画素のモノクロームデジタル画像になると仮定しよう。我々は、これを、これが前記定義における“オリジナル信号”と同一であることを表す“オリジナルデジタル画像”と呼ぶ。

【0050】

走査処理の間、我々は、デジタル値“3.0”に対応する絶対的な照度を任意に設定する。我々は、オリジナルデジタル画像において存在する基本2デジタル数乗ノイズに加えて、所定の画素の輝度値の平方根の理論上のノイズ（産業界において“ショットノイズ”として知られている）が存在することを見聞する。式において、我々は、

$$\langle \text{RMS Noise}_n \rangle = \sqrt{4 + (V_n - 3.0)} \quad (1)$$

を有する。ここで、nおよびmは、画像の行および列において0から3999まで変動する簡単な表示値である。Squareは、平方根である。Vnは、オリジナルデジタル画像における所定の表示画素のDNである。RMSnoiseの範囲のこの括弧は、これが期待される平均値であることを単に意味し、ここで各々すべての画素が、ランダムエラーを個別に有することは明らかである。したがって、デジタル数または“輝度値”として12.0を有する画素値に対して、我々は、その期待される実効ノイズ値がsquare(12.0

4) = 3.4, 7.0 であることが分り、この値は、1200の平方根である34.64にまったく近い。

[0051]

我々はさらに、直素の固有の輝度値の平方根が、正確に equal の不安定ノイズとして知覚する値ではないことを理解しており、したがって我々は、式、

$$\text{Addable Noise}_{i,j} = \sqrt{X^2 + (V_{i,j} - 3.0)^2} \quad (2)$$
 を提案する。ここで、XおよびYを、我々が調節する経験的なパラメータとして加えており、"addable"ノイズは、上述した定義による我々の許容しうる知覚されるノイズレベルに属するものである。我々はここで、我々が選択することができXおよびYの正確な値はどの位なのかを実験しようと思うが、我々は、我々が処理の次のステップを実行すると同時に、

[0052]

我々の処理の次のステップは、我々のNビット検証ワードのNを選択することである。我々は、65536の可能な値を有する16ビット主検証値が、真値が我々のものであることを検証するのに十分に大きく、我々が、我々が追跡を望む画素の128のコピーのみを直接販売すると決定し、7ビットに、最初の7ビットの奇数/偶数の加算（すなわち、最初の7ビットにおけるビットのエラー割合）用の第8ビットを加える。ここで必要な全体のビットは、0101キャリブレーション配列用4ビットと、主検証用16ビットと、バージョン用8ビットとであり、我々はここで、最初の28ビットにおける他のエラー割合として他の4ビットを投入し、Nとして32ビットを与える。最後の4ビットは、その4ビットを選択するために、多くの業界標準エラー割合方法の1つを使用することができる。

[0053]

我々はここで、16ビット主検証値をランダムに決定し、例として、1101 0001 1001 1110を得る。販売されたオリジナルの我々の第1のバージョンは、バージョン識別子としてすべて0を有し、エラー割合ビットは一致しなくなる。我々はここで、我々がオリジナルデジタル画像に埋め込む我々の固有32ビット検証ワードを有する。

[0054]

これを行うために、我々は、我々の32ビット検証ワードの各々のビットに対して、32の独立したランダムの4000×4000の符号化画像を発生する。これらのランダム画像を発生する方法を示す。これらを発生する極めて多くの方法が存在する。明らかに最も簡単な方法は、オリジナル写真における走査に使用される同じスキャナにおいて、入力としてこの時だけ低い画素を置き、次にこれを32回走査することによってゲインを上昇させることである。この技術の欠点は、大容量のメモリが必要なことと、"固定パターン"ノイズが、各々の独立"ノイズ画像"の一部となることだけである。しかし、固定パターンノイズを、通常の"ダークフレーム"減算技術によって除去することができる。我々は、通常ゲイン設定において2DN実効ノイズを見つけるよりもむしろ、絶対黒平均値をデジタル数"100"において設定すると仮定し、ここで我々は、各々すべての直素の平均値について10DNの実効ノイズを見つける。

[0055]

我々は次に、中間空間周波数バンドパスフィルタ（空間粗素）を、各々すべての独立ランダム画像に用い、これらから極めて高い空間周波数と極めて低い空間周波数とを本質的に除去する。我々は、幾何学的歪みや、スキャナにおける汚れや、整合誤りのような簡単な現実世界のエラー源の大部分は、より低い周波数において現れ、我々は、これらの形式の改ざんを回避するために、より高い空間周波数における我々の検証信号に集中したい。ため、極めて低い周波数を除去する。同様に我々は、所定の直素の多数の世代のコピーや圧縮一伸長実験は、より高い周波数をどんな方法でも破壊する傾向があり、これらの周波数が最も破壊する傾向がある場合、これらの周波数中に多すぎる検証情報が位置する点が存在しないようにするために、より高い周波数を除去する。したがって、我々の新たな描

出された独立ノイズ画像は、中央空間周波数によって支配される。実質的な特徴において、我々は我々のスキマヤにおいて12ビット値を使用し、我々はDC値を効果的に除去し、我々の新たな実効ノイズは10デジタル数より僅かに少ないことから、これを、結果として得られるランダム画像として-32から0を通して31まで変動する6ビット値に圧縮することが有効である。

[0056]

次に我々は、対応する32ビット独立検証ワードのビット値において1を有するランダム画像のすべてを互いに加算し、16ビット署名整数画像における結果を蓄積する。これは、複合埋め込み信号の非線装および非比例バージョンである。

[0057]

次に我々は、式2のXおよびYパラメータを変化させることによって、複合埋め込み信号をオリジナルデジタル画像に加えることによって視覚的に実験する。式において、我々は、以下の式においてXの最大化と適切なYを見つけることを繰り返す。

$$V_{\text{distortion}} = V_{\text{distortion}} + V_{\text{distortion}} * X * \text{sqrt}((H_{\text{distortion}} - Y)) \quad (3)$$

ここで、distは候補配布可能画像に適用し、すなわち我々は、我々に許容しうる画像を与えるXおよびYを見つけることを視覚的に繰り返し、origはオリジナル画像の画素値に適用し、compを複合画像の画素値に適用する。nおよびmは、画像の行および列を依然として示し、この操作を4000×4000画素の全てにおいて行うことを示す。符号Vは、所定の画素および所定の画像のDNである。

[0058]

ここで任意の仮定として、我々は、我々の視覚的実験が、オリジナル画像を候補配布可能画像と比較した場合、X=0.025およびY=0.6の値が許容しうる値であることを発見したと仮定する。すなわち、“追加ノイズ”を有する配布可能画像は、美的センスにおいてオリジナルに許容しうるほど近い、我々の独立ランダム画像が10DN程度のランダム実効ノイズ値を有し、16程度のこれらの画像を互いに加算することが複合ノイズを40DN程度に増加させることから、0.025のX増加値が、追加の実効ノイズを1DN程度またはオリジナルにおける我々の固有ノイズの振幅の半分に戻すことに注意されたい。これは大雑把に言って、低い画素値のノイズにおける1dBであり、0.6のY値によって変化したより明るい画素においてより高い値に対応するものである。

[0059]

このようにこれらのXおよびYの2つの値によって、我々はここで、我々のオリジナルの配布可能コピーの第1バージョンを構成する。他のバージョンは、単に新たな複合信号を形成し、必要だと考えるならXを僅かに変更する。我々はここで、オリジナルデジタル画像を、各々のバージョン用32ビット検証ワードと、32の独立ランダム4ビット画像と共に固定し、我々のオリジナルの疑わしい著作権侵害者の我々の最初のケースを待つ。記憶方法、これは、オリジナル画像用に14メガバイト程度、ランダム検証埋め込み画像用に32×0.5バイト×16000000=256メガバイト程度である。これは、1つの高価な画像に関して完全に許容しうる。多少の記憶装置の節約は、簡単な無損失圧縮によって得ることができる。

[0060]

我々の画像の疑わしい著作権侵害の発見

我々は、我々の画像を販売し、数ヶ月後、見たところは我々の画像から切り取られ剥離され、他の様式化された背景画面に置かれたものを見つける。この新たな“疑わしい”画像は、所定の雑誌出版の1000000コピーにおいて印刷されているとする。我々はここで、我々のオリジナル画像の一部が許可されない方法で実際に使用されているかどうかを決定しようとする。図3は、詳細を要約する。

[0061]

第1のステップは、前記雑誌の発行物入手し、前記画像をその上に有するページを切り取り、この時、慎重に、しかし慎重に成り過ぎずに、普通の紙を使用して背景画面から2つの図を切り取ることである。もし可能なら、我々は、2つの図を別々に切り取るより

も、1つの接続された部分のみを切り取る。我々は、これを黒い背景上に張り付け、このことは、視覚的検査を行うのを簡単にする。

【0062】

我々はここで、我々の安全が保証された場所からオリジナルデジタル画像を32ビット検証ワードおよび32の独立埋込み画像と共に得る。我々は、オリジナルデジタル画像を、標準画像操作ソフトウェアを使用する我々のコンピュータスクリーン上に配置し、我々は、疑わしい画像の我々のマスクされた領域と同じ境界線に沿っておおまかに切断し、同時に同じ様にこの画像をおおまかにマスクする。“おおまか”という言葉を、正確な切断が必要でないことから使用し、これは単に検証統計が合理的に棄てられるのを助ける。

【0063】

次に我々は、マスクされた疑わしい画像を再スケーリングし、我々のマスクされたオリジナルデジタル画像の寸法に大まかに適合させる。すなわち我々は、疑わしい画像を拡大または縮小し、それをオリジナル画像の上に大まかに重ね合わせる。我々がこの大まかな整合を行った後、我々は次に、これらの2つの画像を、自動化されたスケーリングおよび整合プログラムに投入する。このプログラムは、x位置、y位置および空間スケールの3つのパラメータを探索し、2つの画像間の二乗平均されたエラーが、なんらかの所定のスケール変数とxおよびyオフセットとで与えられるという形態の利点を有する。これは、全く標準的な画像処理方法論である。代表的に、これを、大体において滑らかな補完技術を使用して行い、サブ画素精度に行う。探索方法を、多くのものの1つとすることができ、シンプレックス方法を代表的な1つとする。

【0064】

最適なスケーリングをし、x-y位置変数を見つけたら、次に、前記2つの画像の黒レベルと輝度ゲインとガンマとの最適化における他の探索を行う。再び使用するべき利点の形態は、二乗平均エラーであり、再びシンプレックスまたは他の探索方法論を、これら3つの変数の最適化に使用することができる。これらの3つの変数を最適化した後、我々は、これらの修正を疑わしい画像に用い、それを、オリジナルデジタル画像およびそのマスクの画素間隔およびマスキングとに正確に整合させる。我々はここで、これを基準マスクと呼ぶことができる。

【0065】

次のステップは、新たに規格化された疑わしい画像から基準マスク領域内のみオリジナルデジタル画像を減算することである。この新たな画像を、差画像と呼ぶ。

【0066】

次に、32の独立ランダム埋込み画像すべてに載って、マスクされた差画像とマスクされた独立埋込み画像との間の局所相関を行う。“局所”を、上述した探索手順中、発見された2つの画像の名目上の整合点間のオフセットの+/-1画素のオフセット領域によって相関させるのを開始することのみが必要であるという観点に適用する。相関のピークを、0、0オフセットの名目上の整合点に極めて近づくべきであり、我々は、3×3相関値を互いに加算し、我々の32ビット検証ワードの32の独立ビットの各々に対する1つの総括的な相関値を与えることができる。

【0067】

すべての32ビット位置とこれらの対応するランダム画像のすべてにこれを行った後、我々は、32値の準浮動小数点配列を有する。最初の4値は、0101の我々のキャリアレシオ信号を表す。我々はここで、第1および第3浮動小数点値の平均を取り、この浮動小数点値を“0”と呼び、第2および第4値の平均を取り、この浮動小数点値を“1”と呼ぶ。我々は次に、残りのすべての28ビット値に進み、単にこれらより近い平均値に基づいて“0”または“1”のいずれかを割り当てる。簡単に言うに、疑わしい画像が実際に我々のオリジナルのコピーの場合、期待される32ビット結果ワードは、我々の記録のそれと一致すべきであり、それがコピーでない場合、我々は全体的なランダム状態を得るべきである。33コピーであるが検証番号と一致しない第3の可能性と、41コピー

ではないが適合する第4の可能性があり得る。3)の場合において、処理の信号ノイズ比が重圧を受け得る。すなわち「疑わしい画像」が正確にオリジナルの極めて重要なコピーである場合があり得る。4)の場合において、我々が3ビット検証番号を使用していることから基本的に40億に1つの可能性がある。我々が4)を本当に心配する場合、我々は、同じ難題の異なる例においてこれらのテストを行う第2の独立した試験場を単に有することができる。最後に、これらの値が何を与えるのかを考慮したエラーチェックビットの割合は、処理全体において最終的な出来るかぎり過剰な検査である。ノイズに対する信号が問題に成りうる状況において、これらのエラーチェックビットを、多すぎる事なしに除去することができる。

【0068】

信益

第1の実施例の完全な説明を、詳細な例によって記述した今、処理ステップとこれらの利点との理論的解釈を指摘することが適切である。

【0069】

前述の処理の最終的な利益は、検証番号を得ることが、差画像を準備する手段および方法と完全に独立していることである。すなわち、切断、整合、スケールリング、等のような差画像の準備の方法は、検証番号が存在しない場合、検証番号を発見するオッズが増加せず、真の検証番号が存在する場合、検証処理の信号ノイズ比のみが役に立つ。検証用画像を準備する方法は、互いに異なっているかもしれず、一致を形成する多数の独立した方法論の可能性を提供する。

【0070】

オリジナル信号または画像の部分集合において一致を得る能力は、今日の情報に富んだ世界におけるキーポイントである。画像および音声部分の双方の切断および振り付けは、より一般的になり、このような実施例をオリジナル作品が不正に使用されている場合、コピーを検出するのに使用させる。最後に、信号ノイズ比の一致は、コピー作品それ自身がノイズまたは隠蔽な歪みのいずれかによって隠蔽に変化している場合のみ困難となり、これらの双方がコピーの商業的価値に影響し、その結果、このシステムを妨げようとすることは、商業的価値における費用の莫大な減少におけるのみ行うことができる。

【0071】

本発明の初期の概念は、1つのみの「スノー状」画像またはランダム信号をオリジナル画像に付加する場合、すなわち $N=1$ の場合であった。この信号を「複合化」することは、この信号の存在または不在における判断を行う（一般的に統計的）アルゴリズムを使用する、その後の数値的解析を含む。このアプローチを上記した実施例として放棄した理由は、前記信号の存在または不在の検出の確実性において固有の灰色領域が存在することである。「0」から「1」の間で選択する方法を規定する簡単な予め規定されたアルゴリズムと組み合わせた多数のビット段階すなわち $N>1$ の前方への変化によって、本発明は、専門的な統計的解析から、コイン投げのようなランダム2値事象を規定する分野に、確実な変化を変化させた。これは、裁判所および市場の双方における本発明の直観的な許容に開係する有力な特徴として見られる。この全体の問題に対する発明者の考えを要約する類似は、次のようなものである。1つの検証番号の検出は、コイン投げを1回のみコールし、このコールを行うことを秘密の専門家に開示することに等しいが、本発明の上述した $N>1$ の実施例は、コイン投げを N 回連続して正確にコールする明白に直観的な原理に期待する。この状況は、非常に可立たせるものであり、すなわち、画像および音声部分がより小さい範囲を得た場合、1つの信号の存在の「改ざん」の問題である。

【0072】

$N>1$ の場合が $N=1$ の実施例よりも好適な実施例である他の理由は、 $N=1$ の場合において、疑わしい画像を準備し操作する方法が、正の検証を行う可能性を得ることである。したがって、専門家が検証の決定を行う方法は、その決定に必須の部分となる。この決定を行う多数の数値的および統計的アプローチの存在は、いくつものテストが正の決定を行い、一方他のテストが負の決定を行うという可能性を残し、種々の検証アプローチの相

対的な利点についての他の秘密の議論をもたらす。本発明のN>1の好適実施例は、既知の個人コード信号を不正に使用する前処理以外に信号の前処理なしで“コイン”投げるN回連続してコールする。可能性を増加することができる方法を提供することによって、この他の灰色領域を回避する。

【0073】

本システムの最も完全な説明は、業界標準および多数の独立したグループが、埋め込み検証番号の適用およびその解読における彼ら自身の手段または“企業内ブランド”を設定するようになる場合、見えてくるだろう。多数の独立したグループ検証は、本方法の最終的な目的をさらに強化し、これによって業界標準としての魅力が増強される。

【0074】

複合埋め込みコード信号の生成における真の極性の使用

上述した論考は、その目的を実行するためにバイナリ技術の0および1の形式論を使用した。特に、Nビット検証ワードの0および1は、これらの対応する独立埋め込みコード信号に直接乗算され、複合埋め込みコード信号を形成する（ステップ8、図2）。このアプローチは、その観念の簡単さを確かに有するが、埋め込みコードの記憶と共に埋め込みコード信号の0による乗算は、一種の非効率性を含む。

【0075】

Nビット検証ワードの0および1の性質の形式論を保持するか、これらの対応する埋め込みコード信号を減算させるワードの0を有することが好適である。したがって、図2のステップ8において、Nビット検証ワードにおいて“1”に対応する独立埋め込みコード信号を“加算”するだけよりも、Nビット検証ワードにおいて“0”に対応する独立埋め込みコード信号の“減算”も行う。

【0076】

一見して、これは、最終的な複合信号により明白なノイズを付加しているように見える。しかし、0から1へのエネルギー幅分離は増加し、したがって図2のステップ10において使用される“ゲイン”を、相対して低くすることができる。

【0077】

我々は、この改良を、真の極性の使用と呼ぶことができる。この改良の主な利点を、“情報の効率”として大きく要約することができる。

【0078】

独立埋め込みコード信号の“短波の直交性”

上述した論考は、一般にランダムノイズ状信号を独立埋め込みコード信号として使用することを考察した。これは、発生する信号の恐らく最も簡単な形式である。しかしながら、独立埋め込み信号の組に用いることができる情報最適化の形式が存在し、本出願人は“短波の直交性”という題目の下に記述する。この用語は、この直交性が、検証情報の信号エネルギーを最大化すると同時に、ある知覚しうるしきい値より下に保持すべきであるという現在の追加の要求による。ベクトルの直交性の数値的な観念に大まかに基づいている。他の方法において、埋め込みコード信号は、必然的に現実ランダムであることを必要としない。

【0079】

露光乳剤ベースの写真の領域における第1実施例の使用および改良

上述した論考は、写真作品に適用できる技術を概説した。以下の節は、この領域の詳細をさらに説明し、これら自身を広範囲な用途に適合させるいくらかの改良を開示する。

【0080】

論考すべき第1の領域は、ネガフィルム、プリント紙、トランスベアレンシスのような慣習的な写真作品上に通し番号を前記入または前露光することを含む。一般に、これは、光学的に固有な通し番号（および金荷的に所有権およびトラッキング情報）を写真作品中に埋め込む方法である。通し番号それ自体は、余白に違いやられるか、プリントされた写真の背景上にスタンプされるのに対比して、通常の露光された画像の組的な部分であり、コピーと別の位置と別の方法とを必要とする。ここで呼ぶ“通し番号”は、一般にNビ

ット検証ワードと同義語であり、ここでのみ我々は、より一般的な業界用語を使用している。

【0081】

図2のステップ11において、本明示は、“オリジナル（真像）”をコード画像とともに記憶することを命じる。次に図3のステップ9において、疑わしい画像からオリジナル画像を減算し、これによって、可能な検証コードにノイズおよび改ざんが蓄積されたもののすべてを加えたものか残るよう命ずる。したがって、以前の開示は、複合埋込み信号なしにオリジナルが存在するという確実の仮定をおこなった。

【0082】

ここで、プリント紙および他のコピー製品を販売する場合において、これは依然としてこの場合、すなわち“オリジナル”が埋込みコード無しに実際に存在し、第1実施例の基本的な方法論を用いることができる。オリジナルフィルムは、“非符号化オリジナル”として完全に良好に役立つ。

【0083】

しかしながら、前露光されたフィルムを使用する場合において、複合埋込み信号がオリジナルフィルム上に予め存在し、したがって予め埋め込まれた信号と分離し、“オリジナル”は、決して存在しない。しかしながら、この後者の場合は、上記で説明した原理をどのように最適に使用するかについての観察とともに、ビットをより厳密に調査する（前者の場合は前記で概説した方法に固執する）。

【0084】

予め番号付けられたネガフィルム、すなわち、各々すべてのフレームに極めて微かな固有複合埋込み信号を前露光されたネガフィルムの場合の変更の最も明白な点は、以前示した図3のステップ4において現れる。他の相違が確かに存在するが、信号をフィルム上にどの様に何時埋め込むか、コード番号および通し番号をどの様に記録するか、等のような視覚的主として論理的なものである。明らかに、フィルムの前露光は、フィルムの生成および包装の一般的な大量生産工程に大きな変化をもたらす。

【0085】

図4は、フィルムを前露光する1つの可能性のあるこれ以後の機構の概念的な電図である。“これ以後”を、すべての共通製造工程をすでに行った後に処理を行うことに適用する。結局、経済的規模が、この前露光工程をフィルム製造の連鎖中に直接に配置することを要求する。図4に示すものは、フィルム書き込みシステムとして既知である。コンピュータ106は、図2のステップ8において生成される複合信号をその露光スクリーン上に表示する。次にフィルムの所定のフレームを、この露光スクリーンの像を映すことによって露光し、このときの露光レベルを一般的に極めて微かに、すなわち一般的にごく僅かにする。明らかに、市場が、これをどの位微かにすべきかの市場自身の要求、すなわち弁護士が見積もる加えられた“性質”のレベルを設定するであろう。フィルムの各々のフレームを、逐次的に露光し、一般にCRT102において表示される複合画像を各々すべてのフレーム毎に変化させ、これによってフィルムの各々のフレームに異なった通し番号を与える。変換レンズ104は、フィルムフレームの焦点変化面とCRT表面とを強調する。

【0086】

前露光ネガフィルムの場合における前述の実施例の原理の適用に戻ると、図3のステップ4において、“オリジナル”をその埋込みコードとともに減算すると、コードがオリジナルの露光部分であることから、明らかにコードも同様に“消去”する。遅長く、経済的規模が存在し、検証を依然として行うことができる。しかしながら、この実施例を改良する技術者は、前露光ネガの場合における検証処理の信号ノイズ比を、非符号化オリジナルが存在する場合の信号ノイズ比に近づくことを要求される。

【0087】

この問題の簡単な定義は、この点における順番である。疑わしい写真（信号）を特定した場合、コードがどこかに存在する場合、埋込み検証コードを見つける。この問題は、上述したようなノイズおよび改ざんの状況内だけでなく、ここでは取り戻された画像とコ

ードとの間の結合の状況内でも、疑わしい写真内の各々すべての独立理の込みコード番号の振幅の発見の1つに減少する。“結合”を、ここでは取り込まれた画像が相同に“ランダムにバイアスする”という概念に適用する。

【0088】

このように、信号結合のこの追加の項目を心に止めておく、検証原理は、各々すべての独立理の込みコードの信号振幅を見積もる(図3のステップ12では相同結果を得るのに対して)、我々の検証コードが疑わしい写真中に存在する場合、発見される振幅は、“1”を割り当てられている正振幅と“0”を割り当てられている負振幅を有する再振幅に分割されている。我々の固有検証コードは、それ自身を明らかにする。他方で、このような検証コードが存在しない場合、または何か他のコードである場合、振幅のランダムガウス分布は、僅のランダムな寄せ集めによって見つかる。

【0089】

独立理の込みコードの振幅をどの様に見出すかについてのいくつかの更なる詳細を与えることが執っている。再び、運良く、この厳密な問題は、他の技術上の用途において見理されている。さらに、この問題と少しの史料とを数学者と統計学者とで組み合わせているいる振幅に投げ込めば、ある適当な期間の後、半タスの最適化された方法論が必ず出で来るであろう。それは、ある程度さらいに定義された問題である。

【0090】

ある特別な例としての解決法は、天文学上の画像の分野から生じる。ここで、成熟した先行技術は、“熱ノイズフレーム”を物体の所定のC D D画像から減算する。しかしながらしばしば、熱フレームの減算においてどの位のスケールリング係数を使用するのが明確に既知ではなく、正確なスケールリング係数の探索が行われる。これは、明確に本実施例のこのステップの仕事である。

【0091】

一般的な習慣は、単に一般的な探索アルゴリズムをスケールリング係数において行い、スケールリング係数を選択し、新たな画像を、

新たな画像=獲得された画像-スケールリング係数×熱画像 (4)

によって形成する。

【0092】

新たな画像に高速フーリエ変換ルーチンを用い、最終的に、新たな画像の積分高周波内容をも最小化するスケール係数を見つける。この個々の量の最小化による一般的な形式の探索操作は、非常に一般的である。したがって発見されたスケール係数は、探索された“振幅”である。考察されているかまた実現されていない改良は、獲得された画像のより高い導関数と埋め込みコードとの結合を、見積もり、計算されたスケール係数から除去することである。すなわち、上述した結合による特定のバイアス効果が存在し、最終的には理論上および経験的な実験の双方によって明らかにされ除去されるべきである。

【0093】

信号または画像の変化の検出における使用および改良

全体として信号または画像を検証することの基本的な必要性から離れて、信号または画像に対して起こりうる変化を検出する多少異なる必要性も存在する。以下の節は、前記実施例を、特定の改良および改良によって、この領域における有効な道具としてどのよう可以使用することができるかを記述する。

【0094】

最初に要約するために、我々は、前記で概説した基本的な方法を使用して正に検証された所定の信号または画像を有すると仮定する。すなわち、我々は、そのNビット検証ワードと、その独立理の込みコード信号と、その複合理の込みコードとを知っている。次に我々は、我々の所定の信号または画像内の複合コードの振幅の空間マップを全く簡単に形成することができる。さらに我々は、規格化マップ、すなわちある大域的平均値の関数を表変するマップを形成するために、この振幅マップを既知の複合コードの空間振幅によって分割することができる。このマップの簡単な調査によって、我々は、明白に変化して、規格

化振幅の値が代表的なノイズおよび改ざん（エラー）に準に基づくしきい値のある統計上の組より低下するなどの様な領域も、視覚的に検出することができる。

【0095】

振幅マップの形成の実施の詳細は、種々の選択を有する。1つは、上述した信号振幅の決定に使用したのと同じ手順を行うことであり、ここでは我々は、我々が調査している領域付近に中心が位置する正規重み関数を信号／画像のすべての所定の領域に集算する。

【0096】

万能コード対カスタムコード

本明細書は、ここでは、各々すべてのソース信号が独立埋め込みコード信号の自分自身の組をどのように有するのかを概説した。これは、オリジナルに加えて相当量の追加のコード情報の記憶を必要とし、多くの用途には、より経済的な形式が適切であろう。

【0097】

あるこのような節約のためのアプローチは、一組のソース作品に共通の独立埋め込みコード信号の所定の組を有することである。例えば、我々の1000枚の画像がすべて、独立埋め込みコード信号の同じ基本的な組を利用することができる。このときこれらのコードに必要とされる記憶は、ソース作品に必要とされる記憶全体のほんの一部となる。

【0098】

さらに、いくつかの用途は、独立埋め込みコード信号の万能組、すなわち配布された作品のすべての場合に同一のままであるコードを利用することができる。この形式に必要なものは、Nビット検証ワードそれ自身を隠そうとし、このワードを読み取ることができる統一された装置を有するシステムによって分かるであろう。これを、読み取り位置の点において判断する／しないシステムにおいて使用することができる。この設定をする潜在的な欠点は、万能コードは、より追跡または盗難されやすく、したがってこれらは、前記で開示した設備の装置および方法論より安全ではない。恐らくこれは、“高い安全性”と“気密の安全性”との間の差であり、潜在的な用途の大部分にとってはあまり重要でない区別である。

【0099】

大規模埋め込みコードを付けることができる紙、文書、プラスチック加工身分証明カード、および他の材料への印刷物における使用

用語“信号”を、デジタルデータ情報、オーディオ信号、画像、等を指示するためにしばしば狭義において使用する。“信号”のより広義の解釈と、より一般的に意図されたものとは、どの様な材料のどの様な形式の変化も含む。したがって、一般的な紙の断片のマイクロトポロギーは、信号（例えばマッシュ座標の関数としての高さ）となる。プラスチックの平坦な断片の屈折特性は、（空間の関数としての）信号となる。要点は、写真感光孔刷、オーディオ信号、およびデジタル化情報は、本発明の原理を使用することができる信号の唯一の形式ではないということである。

【0100】

適切な場合として、ブライユ点字印刷機械に大変よく似た機械を、前記で概説した固有の“ノイズ状”検証を付けるように設計することができる。これらの検証を、ブライユ点字の形成において加えられるよりはるかに小さい圧力によって、そのパターンが置換の普通の使用者によって認められないような位置に加えることができる。しかし、本明細書のステップを続け、微細な検証の機構によってこれらを用いることによって、固有検証コードを、日常の使用としての目的を意図したもので、重要な文書、法的な提出物、または他の保証された作品である、どのような紙面にも配置することができる。

【0101】

このような実施例における検証作品の読み取りは、一般的に、文書を光学的に種々の角度において準に読み取ることによって行われる。これは、紙面のマイクロトポロギを推論するために安楽な方法となる。種々に紙のトポロギを読み取る他の形式も可能である。

【0102】

例えば運転免許書である身分証明カードのようなプラスチックに封入された作品の場合

において、同様のプライム点字印刷機械に類似した機械を、固有検証コードを付けるのに利用することができる。感光材料の薄い層をプラスチックの内部に埋め込み、“感光”させることもできる。

[0103]

“ノイズ域”信号によって変動させることができる材料が存在するところならどこでも、この材料は、固有検証コードおよび本発明の原理を利用するための適切なキャリアとなることは明らかである。経歴的に検証情報を付加し、信号レベルを各々すべての用途がそれ自身に対して規定する許容しうるしきい値より下に保持する問題が現れる全てである。

[0104]

リアルタイムエンコーダ

実施例の第1の組は、画像または信号の符号化を行う標準的なマイクロプロセッサまたはコンピュータを最も一般に使用し、代表的なフォンノイマン型プロセッサより速くすることができるカスタム符号化装置を使用することができる。このようなシステムを、すべてのモードのリアルデータストリームに使用することができる。

[0105]

音楽およびビデオテープ記録を、リアルデータストリーム、しばしば著作権保護を受けるデータストリームの例とする。許可された記録を検証データによって符号化し、著作権侵害された品物をこれらが形成されたものからオリジナルを探索できるようにしたならば、実施の試みの助けとなるであろう。

[0106]

著作権侵害は、本発明を必要とすることの1つにすぎない。他の事は、認定である。しばしば、データの所定の組が（しばしばその発生から数年後）実際に何を意図しているのかを確認することが重要になる。

[0107]

これらおよび他の必要性を説明するために、図5のシステム200を使用することができる。システム200を、検証符号化ブラックボックス202として考えることができる。システム200は、（後に“マスタ”または“非符号化”信号と呼ばれる）入力信号およびコードワードを受け、検証符号化出力信号を（一般にリアルタイムで）発生する。（通常、本システムは、後の復号化に使用するキーデータを提供する）。

[0108]

“フラックボックス”202の中身は、種々の形態をとることができる。典型的なブラックボックスシステムを図6に示し、これは、参照表204と、デジタルノイズ源206と、第1および第2スケアラ208および210と、加算器/減算器212と、メモリ214と、レジスタ216を含む。

[0109]

（図示した実施例においては、1000000標本毎秒のレートにおいて供給される8〜20ビットデータ信号であるが、他の実施例においては、適切なA/DおよびD/Aコンバータが設けられている場合、アナログ信号とすることができる）入力信号を、入力端子218から参照表204のアドレス入力端子220に供給する。各々の入力標本（すなわち、参照表アドレス）に対して、参照表は、対応する8ビットデジタル出力ワードを供給する。この出力ワードを、第1スケアラ208の第1入力端子に供給されるスケアラ値として使用する。

[0110]

第1スケアラ208は、第2入力端子を有し、この入力端子にノイズ源206から8ビットデジタルノイズ信号を供給する。（図示した実施例において、ノイズ源206は、アナログノイズ源222およびアナログ→デジタルコンバータ224を具えるが、再び、他の手段を使用することができる。）図示した実施例におけるノイズ源は、50から100のデジタル数（例えば、-75から+75）の半値全幅（FWHM）を有する、ゼロ平均出力値を有する。

[0111]

第1スケラ208は、その入力端子における2つの8ビットワード(スケラ係数およびノイズ)を乗算し、システム入力信号の各々の標本に対して、1つの16ビット出力ワードを発生する。ノイズ信号がゼロ平均値を有することから、第1スケラの出力信号も同様にゼロ平均値を有する。

[0112]

第1スケラ208の出力信号を、第2スケラ210の入力端子に供給する。第2スケラは、大域的スケラリング機能を行い、最終的に入力データ信号中に埋め込まれる検証信号の絶対量を確立する。前記スケラリング係数を、スケラ制御装置226(簡単な加減算回路から、グラフィカルユーザインタフェースにおいて図式的に実現された制御まで、多くの形態をとることができる)によって設定し、別様の用途の要求にしたがって変更すべきこの係数を可能にする。第2スケラ210は、その出力ライン228にスケラノイズ信号を発生する。このスケラノイズ信号の各々の標本を、メモリ214に順次記憶する。

[0113]

(図示した実施例において、第1スケラ208からの出力信号は、 -1500 と $+1500$ (10進数)との間で変化するが、第2スケラ210からの出力信号は、小さい1つの数字である(-2 と $+2$ の間のような))。

[0114]

レジスタ216は、多ビット検証コードワードを記憶する。図示した実施例において、このコードワードは、8ビットから成るが、より大きいコードワード(数100ビットに及ぶ)が一般的に使用される。これらのビットを一度に1つ参照し、入力信号のスケラノイズ信号による変動の程度を制御する。

[0115]

特に、ポイント230を、レジスタ216におけるコードワードのビット位置を通じて順次に循環させ、“0”または“1”の制御ビットを加算器/減算器212の制御入力端子232に供給する。ある入力信号標本に関して、制御ビットが“1”の場合、ライン232におけるスケラノイズ信号標本を入力信号標本に加算する。制御ビットが“0”の場合、スケラノイズ信号標本を入力信号標本から減算する。加算器/減算器212からの出力端子は、ブロック234の出力信号を発生する。

[0116]

コードワードのビットに従ったスケラノイズ信号の加算または減算は、一般にごく僅かな入力信号の変動に影響する。しかしながら、メモリ214の内容の記憶によって、ユーザは、符号化を後に復号化し、オリジナル符号化処理において使用されるコード番号を決定することができる。(実際に、メモリ214の使用は、以下に説明するように任意である)。

[0117]

符号化信号を、印刷された画像に変換された形式、磁気媒体(フロッピーディスク、アナログまたはDATテープ、等)に記憶された形式、CD-ROM、等々を含むよく知られた方法において配布することができることが認識されるだろう。

[0118]

復号化

種々の技術を、疑わしい信号が符号化されているまで検証コードを決定するのに使用することができる。2つを以下で論考する。第1のものは、多くの用途にとって後者よりも好適ではないが、ここで論考することによって、読み手は、本発明を理解するより完全な状況を論考であらう。

[0119]

さらに特に、第1の復号化方法は、差方法であり、オリジナル信号の対応する標本を疑わしい信号から減算し、差標本を得ることによるものであり、次に決定論的に符号化された証印(すなわち、記憶されたノイズデータ)に対して調査する。したがってこのアプローチを、“標本に基づく決定論的”復号化技術と呼ぶことができる。

[0120]

第2の復号化技術は、オリジナル信号を使用しない、個々の標本を調査して、予め決められたノイズ特性を算出することもない、むしろ、疑わしい信号の統計値（またはこれらの一部）を、全体として考え、分析して、信号全体に充満する検証信号の存在を識別する。充満に対する言及は、検証コード全体を、疑わしい信号の小さい部分から識別することができることを意味する。したがってこの後者のアプローチを、“ホログラフィック統計的”復号化技術と呼ぶことができる。

[0121]

これらの方法の双方は、疑わしい信号をオリジナルに整合させることによって開始する、これは、スケージング（例えば、振幅、継続時間、色バランス、等における）と、オリジナルの標本化レートを復旧するための標本化（または再標本化）とを必要とする。上述した実施例におけるように、この整合機能に関連する操作を行うことができる種々の良く理解された技術が存在する。

[0122]

言及したように、第1の復号化アプローチは、オリジナル信号を整合された疑わしい信号から減算し、差信号を残すことによって生じる。次に連続する差信号標本の極性を、対応する記憶されたノイズ標本信号の極性と比較し、検証コードを決定することができる。すなわち、第1差信号標本の極性が第1ノイズ信号標本の極性と一致した場合、検出コードの第1ビットを“1”とする。（このような場合、9番目、17番目、25番目、等の標本の極性も、すべて正とすべきである。）第1差信号標本の極性が、対応するノイズ信号標本の極性と反対である場合、検証コードの第1ビットを“0”とする。

[0123]

差信号の8つの連続する標本について前述の分析を行うことによって、オリジナルコードワードを具えるビットの配列を決定することができる。好適実施例におけるように、符号化中、ポイント230が、コードワードを通して一度に1ビット進み、第1ビットによって開始する場合、差信号の最初の8つの標本を分析し、8ビットコードワードの値を唯一決定することができる。

[0124]

ノイズの無い世界（ここで言っているノイズは、検証符号化に作用するノイズと無関係である）において、前述の分析は、常に正確な検証コードをもたらす。しかし、ノイズの無い世界においてのみ適合した処理は、実際は利用が制限される。

[0125]

（さらに、ノイズの無い状況における信号の正確な検証を、種々の他のより簡単な方法、例えば、チェックサム、すなわち、疑わしい信号およびオリジナル信号間の統計的不可能性一致、等によって処理することができる）。

[0126]

復号化においてノイズが引き起こす異常を、信号の大きな部分を分析することによって、ある程度まで、処理することができるが、このような異常は、処理の信頼性において実際的な上根を依然として設定する。さらに、直視しなければならない意人は、常にランダムノイズより使しくない、むしろ、人間によって引き起こされる形式の改ざん、歪み、不正な操作、等が、益々選択される。このような場合において、検証の信頼性の所望の程度は、他のアプローチによってのみ達成される。

[0127]

現在好適なアプローチ（“ホログラフィック、統計的”復号化技術）は、疑わしい信号を特定のノイズデータ（代表的に、メモリ214に記憶されたデータ）と再結合し、結果として得られる信号のエントロピーを分析することに関する、“エントロピー”を、その最も厳密な数学的定義において理解する必要はなく、単に、ランダム性（ノイズ、平坦性、零特性、等）を記述する最も簡潔な言葉とする。

[0128]

大部分のリアルデータ信号は、ランダムではない、すなわちある標本は、通常、隣接

する標本と、ある程度相関する。対照的に、代表的にノイズは、ランダムである。ランダム信号（例えば、ノイズ）を、非ランダム信号に加算した場合（またはこれから減算した場合）、結果として得られる信号のエントロピは、一般的に増加する。すなわち、結果として得られる信号は、元の信号よりもランダムな偏差を有する。これは、現在の符号化処理によって発生された符号化出力信号の場合であり、元の非符号化信号より大きいエントロピを有する。

【0129】

対照的に、ランダム信号の非ランダム信号への加算（またはこれからの減算）が、エントロピを減少させる場合、なんからの例外が発生する。好適な復号化処理を使用し、埋め込み検査コードを検出することが、この例外である。

【0130】

このエントロピに基づく復号化方法を十分に理解するために、8番目毎に同様の処理であるオリジナル復号化処理の特徴を強調することが第1の助けとなる。

【0131】

前記で論考した符号化処理において、ポイント230は、コードワードを通じて、入力信号の各々の連続する標本毎に1ビット増分する。コードワードが8ビット長の場合、ポイントは、コードワード中の同じビット位置に8番目の標本毎に戻ってくる。このビットが“1”ならば、入力信号にノイズを加算し、このビットが“0”ならば、入力信号からノイズを減算する。したがってポイント230の周期的な進行によって、符号化信号の8番目毎の標本は、特徴を共有し、ポイント230によってアドレスされているコードワードのビットが“1”か“0”に応じて、これらをすべて、対応するノイズデータによって増加するか（反対でもよい）、これらをすべて減少する。

【0132】

この特徴を利用するために、エントロピに基づく復号化処理は、疑わしい信号の8ビット毎に、同様の方法で処理する。特に、疑わしい信号の1番目、9番目、17番目、25番目、等の標本に、メモリ214に記憶された対応するスケールのノイズ信号（すなわち、各々、1番目、9番目、17番目、25番目、等のメモリ位置に記憶されたノイズ信号）を加算することによって、処理を開始する。次に、結果として得られる信号（すなわち、8番目の標本毎に変更された疑わしい信号）のエントロピを計算する。

【0133】

（信号のエントロピまたはランダム性の計算法は、当業者には良く知られている。一般的に受け入れられているものは、各々の標本点において信号の瞬間値を取り、これらの値を二乗し、信号全体に渡って合計することである）。

【0134】

次に、上記のステップを繰り返し、この時、記憶されたノイズ値を、疑わしい信号の1番目、9番目、17番目、25番目、等の標本から減算する。

【0135】

これらの2つの操作の一方は、符号化処理を取消し、結果として得られる信号のエントロピを減少させ、他方は、それを悪化させる。メモリ214中のノイズデータの疑わしい信号への加算が、そのエントロピを減少させる場合、このデータは、以前オリジナル信号から減算されたに違いない。これは、ポイント230が、これらの標本が符号化された時、“0”ビットを指していたことを示す。（加算器/減算器212の制御入力増子における“0”は、スケールノイズの入力信号からの減算を生じる）。

【0136】

反対に、ノイズデータの疑わしい信号の8番目毎の標本からの減算が、そのエントロピを減少させる場合、符号化処理は、以前このノイズを加算したに違いない。これは、ポイント230が、標本1、9、17、25、等が符号化された時、“1”を指していたことを示す。エントロピの減少が、記憶されたノイズデータの疑わしい信号の a からの (a) 加算または (b) 減算のいずれかによるものに注目することによって、コードワードの第1ビットが、 (a) “0”または (b) “1”であるかを決定することができる。

【0137】

上記の操作を、疑わしい信号の第2標本(すなわち、2、10、18、26、...)に始まる一定の間隔をおいた標本のグループに対して行う。結果として得られる信号のエントロピは、コードワードの第2ビットが、“0”または“1”のいずれであるかを示す。疑わしい信号の続く6個のグループに対して同様に、コードワードの8ビットすべてを識別するまで繰り返す。

【0138】

上述したアプローチが、種々の標本の値を変更する改ざん機構に実動されないことは、理解されるであろう。すなわち、代わりに、このアプローチは、信号のエントロピを、結果における高い程度の信頼性を生じるものと見なす。さらに、信号のわずかな故障をこの方法によって分析し、オリジナル著作物の組部の著作権侵害も検出することができる。したがって結果として、疑わしい信号の自然および人的改ざんの双方に直面して、統計的に健全である。

【0139】

さらに、このリアルタイムの実施例におけるNビットコードワードの使用が、パッチ符号化システムに関連して、上述したのと類似の利益をもたらすことが理解されるだろう。(実施例は、本実施例で、パッチ符号化システムにおいて、N標の差ノイズ信号を使用するものとして概念化することができる。第1ノイズ信号を、入力信号と同じ広がりをも有し、標本間0を有する1番目、9番目、17番目、25番目、等の標本(N=8として)におけるスケールノイズ信号を見える信号とする。第2ノイズ信号を、標本間0を有する2番目、10番目、18番目、26番目、等の標本におけるスケールノイズ信号を見える同様の信号とする。その他同様。これらの信号をすべて混合し、複合ノイズ信号を発生する。)このようなシステムにおいて固有の重要な利点の1つは、一致が真に一致である統計的な信頼性(検証コードの各々の連続するビットとともに倍になる信頼性)の程度が高いことである。このシステムは、疑わしい信号の1つの決定論的な埋め込みコード信号に対する主観的な評価に頼らない。

【0140】

説明例の変形例

上述した説明から、示したシステムに対して、基本的な原理を変更することなく、多くの変更を行えることが認識されるだろう。これらの変形例のいくつかを、以下に記述する。

【0141】

上述した復号化処理は、どちらの操作がエントロピを減少させるのかを見つけるために、記憶されたノイズデータの疑わしい信号への/からの加算および減算の双方を試す。他の実施例において、これらの操作の一方のみを行う必要がある。例えば、ある一方の復号化処理において、疑わしい信号の8番目毎の標本に対応する記憶されたノイズデータを、前記標本に加算のみ行う。結果として得られる信号がそのために増加した場合、コードワードの対応するビットは、“1”である(すなわち、このノイズは、以前、復号化処理中に加算されており、再び加算されたために、信号のランダム性のみが増加した)。結果として得られる信号がそのために減少した場合、コードワードの対応するビットは、“0”である。記憶されたノイズ信号を減算するエントロピの他の記憶は、必要ない。

【0142】

検証処理(符号化および復号化)の統計的信頼性を、大域的スケーリングファクタの適切な選択によって、どのような信頼性しきい値(例えば、99.9%、99.99%、99.999%、99.9999%、等)も実質的に越えるように設計することができる。なんらかの所定の用途(大部分の用途においては必要ない)における特約の信頼性を、復号化処理を再検査することによって達成することができる。

【0143】

復号化処理を再検査する一つの方法は、識別されたコードワードのビットに従って疑わしい信号から記憶されたノイズデータを除去し、“復旧”信号を発生する(例えば、コー

下ワードの第1ビットが“1”であることが分かった場合、メモリ214の第1、第9、第17、等の位置に記憶されたノイズ標本を、疑わしい信号の存在する標本から減算する) ことである。記憶されたノイズ信号のエントロピを測定し、他の測定における基準として使用する。次に、この処理を繰り返す。この時、変更されたコードワードに就いて、記憶されたノイズデータを疑わしい信号から除去する。変更されたコードワードは、結合された(例えば、第1)1ビットを除いて、識別されたコードワードと同一である。結果として得られる信号のエントロピを測定し、前記基準と比較する。識別されたコードワードにおけるビットのトランジタが増加されたエントロピを生じる場合、識別されたコードワードのそのビットの精度は、精実になる。トグルされた確認されたコードワードの異なるビット毎に、コードワードのすべてのビットが検査されるまで、この処理を繰り返す。各々の変更の結果として、基準値に比べてエントロピが増加する。

[0144]

メモリ214に記憶されたデータは、種々の二者択一を受ける。上述した論考において、メモリ214は、スケールノイズデータを含む。他の実施例において、非スケールノイズデータを、代わりに記憶することができる。

[0145]

さらに他の実施例において、入力信号それ自身の少なくとも一部を、メモリ214に記憶することが望ましいかもしれない。例えば、このメモリは、8つの著名ビットをノイズ標本に割り当て、16ビットを18または20ビットオーディオ信号標本の最上位ビットの記憶に割り当てることができる。これは、いくつかの利益を有する。1つは、“疑わしい”信号の整合が簡単になることである。他の利益は、既に符号化された入力信号を符号化する場合、メモリ214内のデータを、どちらの符号化処理が最初に行われたかを識別するのに使用することができることである。すなわち、メモリ214内の入力信号データから(不十分にしかかわらず)、一般に、2つのコードワードのどちらが符号化されているかを決定することができる。

[0146]

メモリ214のさらに他の二者択一は、全体を省略できることである。

[0147]

これを達成できる方法の1つは、符号化処理において、既知の鍵番号によって種を確かせるアルゴリズムノイズ源のような決定論的ノイズ源を使用することである。同じ鍵番号によって種を確かせる同じ決定論的ノイズ源を、復号化処理において使用することができる。このような装置において、メモリ214に通常記憶される大きなデータセットの代わりに、後に復号化において使用するために鍵番号のみを記憶する必要がある。

[0148]

代わりに、符号化中加算されたノイズ信号がゼロ平均値を有しておらず、コードワード長さNがデコラックによって既知である場合、万端復号化処理を行うことができる。この処理は、上述した手順と同様のエントロピ試験を使用するが、可能なコードワードを簡略し、試験されているコードワードのビットにしたがって、エントロピの減少が認められるまで、疑わしい信号のN番目の標本内に小さいタミーノイズ値(例えば、予測される平均ノイズ値より小さい)を加算/減算する。しかしながら、このようなアプローチは、他の実施例より低い安全性しか示さない(例えば、野蠻能力によるクラッキングを受けやすい)ため、大部分の用途に対しては好適ではない。

[0149]

多くの用途を、異なるコードワードを使用し、各々が同じノイズデータを使用する。入力信号のいくつかの異なるように符号化された変形を発生する図7に示した実施例によって取り扱うことができる。さらに特に、図7の実施例240は、ノイズ源206からのノイズを、第1コードワードによる入力信号の識別符号化中に記憶するノイズストア242を含む。(図7のノイズ源を、図の筐体上、リアルタイムエンコーダ202の外側に示す。)その後、入力信号の追加の検証符号化版を、前記ストアから記憶されたノイズデータを読み取り、N番目のコードワードを通じて交互に結合し、この信号を符号化すること

によって発生することができる。(2 直進逐次コードワードを図7に示すが、他の実施例においてコードワードの任意の配列を使用することができる。) このような装置によって、比図したサイズのロッキングタムノイズメモリを必要とすることなく、多くの数の異なる符号化された信号を発生することができる。代わりに、一定量のノイズデータを記憶し、オリジナルを1回または1000回符号化する。

【0150】

(もし望むなら、いくつかの異なる符号化された出力信号を、順次ではなく同時に発生することができる。あるこのような実施は、各々が同じ入力信号および同じスケールノイズ信号によって駆動されるが、異なるコードワードによって駆動される複数の加算器/減算器を含む。この場合各々は、異なる符号化された出力信号を発生する) 。

【0151】

同じオリジナルの多くの異なる符号化版を有する用途において、コードワードのすべてのビットを常に調製する必要はないことが認識されるだろう。例えば時々、用途は、疑わしい信号が属するコードのグループのみの検証を必要としてもよい。(例えば、コードワードの高位のビットは、同じソース作品のいくつかの異なる符号化版が発生された構造を示す低位のビットは、特定のコピーを示す。疑わしい信号が関係している構造を検証するために、構造を高位のビットのみにによって検証することができることから、低位のビットを調査する必要はない。) 検証必要条件を、疑わしい信号におけるコードワードビットの部分集合を識別することによって満たすことができるならば、復号化処理を短縮することができる。

【0152】

いくつかの用途を、あるときには異なるコードワードとともに、何回か複分作業中に、符号化処理を再開することによって最適に取り扱うことができる。例として、ビデオテープ作品(例えば、テレビジョン番組)を考える。ビデオテープ作品の各々のフレームを、固有コード番号とともに検証符号化することができ、図8に示したのと同様の装置248によってリアルタイムで処理することができる。垂直解像度をシーク検出器250によって検出する度に、ノイズ源206をリセットし(例えば、丁度発生された配列を繰り返す)、検証コードを次の値に増加する。それによってビデオテープの各々のフレームは、固有に検証符号化される。代表的に、符号化信号を、長期間記憶するためにビデオテープに記憶する(レーザディスクを含む他の記憶媒体も使用することができる)。

【0153】

符号化装置に戻ると、示した実施例における参照表204は、入力データ信号の大振幅の根本は、小振幅入力根本ができるよりも高いレベルの符号化検証符号化を取り扱うことができるという事実を利用する。したがって例えば、0、1または2の10進数値を有する入力データ根本を、1(またはゼロ)のスケール係数に対応させることができるが、200を超える値を有する入力データ根本を、15のスケール係数に対応させることができる。一般的に言って、スケール係数および入力根本値は、平方根関係によって対応する。すなわち、根本値入力信号の値における4つ折の増加は、これらに關係するスケール係数の値における2つ折の増加にほぼ対応する。

【0154】

(ゼロのスケール係数に対する確率的参照として、例えば、ソース信号が時間的または空間的に情報内容が無い場合に言及する。画像において、例えば、いくつかの検出された0の根本値によって特徴付けられる領域を、フレームの真黒領域に対応させることができる。ゼロのスケール係数を、著作権侵害される真黒データが実質的にないことから、ここに充てることができる)。

【0155】

符号化処理を続けると、当業者は、示した実施例における「エラーレー」に対するボテンシャルを認識するであろう。例えば、入力信号が8ビット根本から成り、これらの根本が0から255(10進数)の範囲全体に及んでいる場合、入力信号へのからのスケールノイズの加算/減算は、8ビットによっては表すことができない出力信号(例えば、

一2または257)を発生するかもしれない。この状況を修正する多くの良く理解されている技術が存在し、これらのあるものは順行的であり、これらのあるものは反動的である。これらの両者の技術は共通して、入力信号が0〜4または251〜255の範囲内に標準を持たないようし、それによってノイズ信号による変調を安全に行うが、他にノールエラーを発生する入力信号標本を検出し、適合するように変更する装置を含むのである。

[0156]

示した実施例は、コードワードを逐次に、一度に1ビットずつ進むことを記述するが、コードワードのビットをこの目的のために順次ではなく使用できることが理解できるであろう。実際に、コードワードのビットを、なんらかの予め決められたアルゴリズムに従って選択することができる。

[0157]

入力信号の瞬間の値に基づくノイズ信号の動的なスケールリングは、多くの実施例において省略することができる最適化である。すなわち、参照表204および第1スケラ208を完全に省略し、デジタルノイズ源206からの信号を、加算器/減算器212に直接(または第2大域的スケラ210を通して)供給することができる。

[0158]

さらに、ゼロ平均ノイズ源の使用が示した実施例を簡単にすることが認識されるであろうが、本発明には必要ではない。他の平均値を有するノイズ信号を、容易に使用することができる。(もし必要なら)D、C、補正を、本システム以外で行うことができる。

[0159]

ノイズ源206の使用も任意である。種々の他の信号源を、用途に応じて、初版(例えば、符号化検証信号が知覚できるようにするしきい値)に応じて使用することができる。多くの場合において、埋め込み検証信号のレベルは、検証信号がランダムな状態を有する必要がある。すなわちその性質にもかかわらず知覚できないほど十分に低い。しかしながら、埋め込み検証信号の知覚できないことのレベルに対して、最も大きな検証コード信号S/N比(この場合において、多少不適切な言葉)を提供するため、擬似ランダム源206が通常望ましい。

[0160]

検証符号化を、信号を(すなわち、米国著作権法の言葉において「実際の形式において一定の」)データとしての記憶された形式に減少した後で行う必要はないことが認識されるであろう。例えば、その演奏がしばしば不正に録音される人気音楽家の場合を考える。コンサートホールのスピーカを駆動する前にオーディオを検証符号化することによって、コンサートの認可されない録音を、個々の場所および時間まで追跡することができる。さらに、911非常呼び出しのような生のオーディオ源を、これらの後の認証を容易にするために、録音前に符号化することができる。

[0161]

ブラックボックス実施例を独立型ユニットとして記述したが、多くの道具/器具中に構成要素として統合されることが認識されるであろう。その1つは、検証コードを走査した出力データ中に埋め込むことができるスキヤナである。(これらのコードを、単にこのデータが個々のスキヤナによって発生されたことを記念するために取り扱うことができる)。他のものは、Adobe社、Macromedia社、Corel社、および同様の会社によって提供されている一般向けの描画/グラフィックス/アニメーション/ペイントプログラムのような創造的なソフトウェアにおけるものである。

[0162]

最後に、リアルタイムエンコーダ202を個々のハードウェアの実装の参照とともに説明したが、種々の他の実装を代わりに使用できることが認識されるであろう。いくつかは、他のハードウェア形態を利用する。他のものは、説明した機能ブロックのいくつかまたはすべてに対してソフトウェアルーチンを使用する。(これらのソフトウェアルーチンを、80x86PC互換コンピュータ、RISCベースのワークステーション、等のような

多くの異なった一般的な目的のプログラム可能コンピュータにおいて実行することができる。

【0163】

ノイズ、擬似ノイズ、および普通化ノイズの形式

これまで、本明細書は、直復または信号全体に渡って情報の1ビットを搬送するのに適切な搬送波信号の種類の中のいくつかとして、ガウスノイズ、“ホワイトノイズ”、および用途器具から直接発生されたノイズを仮定した。ある目標を達成するために、ノイズの“設計”特性において、さらに順向的にすることが可能である。ガウスまたは器具ノイズを使用する“設計”は、“絶対的”安全性のためにいくらか向けられている。本明細書のこの節では、検証情報の究極的な搬送波と考えることができるノイズ信号の設計のための、他の考察を調べる。

【0164】

いくつかの用途に関して、搬送波信号（例えば、第1実施例におけるN番目の埋め込みコード信号、第2実施例におけるスカラーノイズデータ）を、検証信号にこの信号の知覚可能性に関してより絶対的な信号強度を与えるために設計することが有利であるかもしれない。ある例は、以下のようなものである。真のガウスノイズは、値“0”が最も頻繁に生じ、次に1および-1が各々等しい確率だが“0”よりは低い確率で生じ、次に2および-2、等々である。明らかに、値0は、本発明において使用されるような情報を搬送しない。したがって、ある簡単な変調または設計は、埋め込みコード信号の発生においてゼロが発生するときはいつもの、新たな思想が引き継ぎ、値を“ランダム”1または-1のいずれかに変換する。このような思想のヒストグラムは、0の値が空であり、1および-1の値が通常の0の値のヒストグラム値の半分だけ増加していることを除けば、ガウス／ポアソン型分布として現れる。

【0165】

この場合において、検証信号エネルギーは、通常、信号のすべての部分において現れる。交換のいくつかは、“決定論的成分”がノイズ信号の発生の一部であるコードの安全性の（大抵、無視できる）低下が存在することを含む。これを完全に無視できる理由は、我々が、1または-1をランダムに選択するコイン投げ形式の状況に依然として準備しているからである。他の交換は、設計されたノイズのこの形式が、知覚可能性の高いしきい値を有し、データストリームまたは両側の最下位ビットが題材の商業上価値に関してすでに無視できる。すなわち、最下位ビットが信号（またはすべての信号根本）から取り除かれた場合、誰もその差を識別できず、題材の価値が損害を受けない用途にのみ使用することができることである。上述した例におけるこのゼロ値の制限は、当業者の誰もが実現できるような信号搬送波のノイズ特性を“最適化”する多くの方法の一つである。我々は、これを、自然ノイズを予め決められた方法においてすべての意図および目的に対してノイズとして読み取られる信号に変換することができるという意味で“擬似ノイズ”とも呼ぶ。暗号化方法およびアルゴリズムが、完全にランダムとして加算される信号を、容易に、そしてしばしば定義によって生成することもできる。したがって、“ノイズ”という言葉は、観察者または聴取者によって主観的に定義されるものと、数学的に定義されるものと間で、異なる意味を有する。後者の違いは、数学的ノイズが、異なった安全性の性質を有し、追跡することができる簡単さか、このノイズの存在を“自動的に認識”することができる簡単さかを有する。

【0166】

“万能”埋め込みコード

本明細書の大部分は、絶対的安全性のために、検証信号の情報のビットを搬送するノイズ埋め込みコードを、各々すべての埋め込み信号に対して固有のものにすべきであるが、わずかに制限を少なくして、埋め込みコード信号を、例えば、フォーマットの1000個の断片の1断片に対して同じ埋め込みコードを使用するように整えめに発生すべきであることを教えている。いずれにせよ、我々が“万能”埋め込みコード信号と呼ぶことができるものを使用することによって、この技術に関して新たな用途を大きく開発することができる他

のアプローチが存在する。これらを使用することの経済性は、これらの万能コードの実際の低い信頼性（例えば、これらは、時間に頼った暗号復号化方法によって分析可能であり、したがって、可能性が殆どなげられるまたは置き換えられる）が、意図された使用を規定した場合の経済的利益と比較して経済的に無視できるようなものである。著作権侵害者および非合法な使用は、単に、予想しうる“費用”および未取収の収入源となり、すなわち全体の経済的分析における簡単なラインアイテムとなる。これの良い例は、ケーブル産業とビデオ信号の成長を減らすことにおけるものである。一般に法律を甘受する市民である狡猾な技術者に熟練した個人が、全ての有料チャンネルをただにするためのケーブル接続ボックスにおいて、梯子をのぼり、教本のワイヤをはきくことができることを誰もが知っていると思われる。ケーブル産業は、これを知っており、それを停止し、隠れたこれらの盗訴する有効な方法を選択するが、この習慣に発する“失われた収入”は、いまだ普及しており、しかしシステム全体をスクランブルすることによって得られる利益の割合としては、ほとんど無視できる。全体としてのスクランブル化システムは、“完全な安全性”の欠陥に陥わず、経済的に成功している。

【0167】

同様なことが、この技術の用途に対して真実であり、ある程度の安全性を低下する価格に対して、大きな経済的機会をそれ自身に与える。この前は、最初に、万能コードによって何がもたらされるかを記述し、次に、これらのコードを用いることができるいくつかの興味深い使用に移る。

【0168】

万能的埋込みコードを一般に、正確なコードの知識を配布することができるという概念に適用する。埋込みコードを、（本明細書の他の部分において言及したように）訴訟がなされるまで決して接触されない秘密の金庫中に置かずに、代わりにその場で分析を行うことができる種々の場所に配布する。一般にこの配布は、安全性が制約された状況に依然として置かれており、ステップは、コードの認識が知ることを必要とするこれらに対して制限されることを意味する。著作権を有する作品を自動的に検出しようとする方法は、コードを知ることを必要とする“何か”の人間でない所である。

【0169】

万能コードの概念を実施する多くの方法が存在し、これらの各々が、何らかの所定の用途に関しては利点を有する。この技術を教える目的のために、我々は、これらのアプローチを3つのカテゴリ、すなわち、ライブラリを基礎とする万能コードと、決定論的公式を基礎とする万能コードと、予め規定された業界標準パターンを基礎とする万能コードとに分類する。おさげなやり方は、第1のものは、後者の2つより安全性が高いが、後者の2つは、第1のものよりもより経済的に実現できるとする。

【0170】

万能コード：1）万能コードのライブラリ

万能コードのライブラリの使用は、固々の埋込みコード信号の制限された組のみが発生し、どのような所定の符号化材料もこの制限された“万能コード”の部分集合を使用することを除いて、本発明の技術を使用することを単に意味する。一例は、以下のものが適切である。写真印刷紙製造業者は、固有検証コードとともに販売したい8×10インチの印刷紙のすべてを前産光することを望むことができる。彼らは、検証コード認識ソフトウェアを、彼らの大口顧客、サービス部、在庫代理店、および個々の写真家に販売し、その結果、すべてのこれらの人々が、かれらの題材が正確にマークされていることを照合できるだけでなく、彼らがまさに得ようとしている第三者の題材がこの技術によって著作権を取得しているとして確認された場合、決定することができるようにすることも望む。この後者の情報は、多くの他の利益のなかで、著作権所有者を確証し、訴訟を無効にするのを助ける。この計画を“経済的に”行うために、各々すべての印刷紙に固有検証埋込みコードを発生することは、情報とは独立に数テラバイトを発生し、これらのバイトを記憶する必要がある。これらのバイトに認識ソフトウェアがアクセスする必要がある。代わりに、彼らは、50個の独立“万能”埋込みコード信号のみの組から得た16ビット検証コ

一下を彼らの印刷紙に埋め込むことを決める。これをどのように行うかについての詳細は、次の節におけるものであるが、これらの認識ソフトウェアが、代表的に 8×10 の印刷紙に印刷された 500×16 の個々の埋め込みコードに対して（デジタル圧縮を考慮して）1メガバイトから10メガバイトの情報である。彼らのコードのライブラリにおける埋め込みコードの制限された値を含むことのみを必要とすることが、ここでの観点である。16の代わりに50を理由は、安全性がわずかに増すためであり、すべての写真に対して同じ16個の埋め込みコードにした場合、シリアル番号容量が2の16乗に制限されるだけでなく、より少ない洗練された著作権侵害者。これらのコードを解読し、ソフトウェアツールを使用してこれらを除去することができる。

[0171]

この計画を実施するための多くの異なった方法が存在し、以下は好適な方法の一つである。企業経営の知識によって、埋め込みコード信号のための1インチ当たり300画素の規準は、多くの用途に関して十分な解像度であると定義される。これは、復号埋め込みコード画像が、 8×10 のシート上に極めて低いレベルにおいて露光すべき 3000×2400 画素を含むことを意味する。これは、 7200000 画素を与える。図4および6のブラックボックス手段において記述したような我々の交互配列符号化システムを使用すれば、各々の独立埋め込みコード信号は、16分の 7200000 すなわち $450k$ 程度の真の情報を搬送する画素、すなわち所定のラスタライン上のすべての16番目の画素のみを含む。これらの値は、代表的に2から2の範囲のデジタル数であり、符号3ビット数によって十分に記述される。このとき埋め込みコードの未加工の情報内容は、 $450k$ の $3/8$ 番目のバイト倍すなわち $170k$ バイト程度である。デジタル圧縮によって、これをさらに減少することができる。これらの決定のすべては、近い将来になんらかの所定の用途によって規定される。本技術分野において既知の、標準工学最適化原理に属する。したがって、我々は、これらの50個の独立埋め込みコードが数メガバイトに達することができる。これは、認識ソフトウェア内の万能コードの“ライブラリ”として配布するために全く適度なレベルである。進歩した標準符号化装置を、自称著作権侵害者が単に万能埋め込みコードをリバースエンジニアするために認識ソフトウェアを購入したことに1つが関係する場合、これらのコードの正確な特徴を隠すために使用することができる。認識ソフトウェアは、本明細書において教えた認識技術を用いる前に、コードを簡単に復号化することができる。

[0172]

認識ソフトウェアそれ自体は、種々の特徴を暗かに有するが、行う中心的な仕事は、所定の画像中にある万能著作権コードが存在する場合、これを決定することである。鍵となる問題は、もしあるとすれば、合計50個の万能コードのうちどの16個が含まれているかということと、16個が見つかった場合、これらのビット値は何かということである。これらの問題の回答の決定における健全数は、整合と、回転と、拡大（スケール）と、範囲とである。助けとなるヒントが何もない大部分の一般的な場合において、すべての変数を、すべての相互結合に就いて独立して変化させるべきであり、50個の万能コードの各々を、エントロピーの減少が発生するかどうかを見つけるために、加算および減算によって検査すべきである。厳密に言えば、これは莫大な仕事であるが、確かなコピーと比較するオリジナル画像を有するような、または 8×10 の印刷紙に比例する画像のオリエンテーションおよび範囲を知るこのような、この仕事をはるかに簡単にする多くの有用なヒントが見つかり、簡単な整合技術によって、ある許容しうる程度に対する変数のすべてを決定することができる。このとき、エントロピーにおけるなんらかの減少を見つけるために、50個の万能コードを通して繰り返すことが単に必要である。1つを行った場合、他の15個を行うべきである。50個の万能コードの所定の順序を、10コードワードの最上位ビットから最下位ビットまでの順序に寛容する設定をするために、プロトコルが必要である。したがって、我々が、万能コード番号“4”の存在を発見し、そのビット値が“0”であることを発見し、万能コード“1”から“3”が明確に存在しないことを発見した場合、我々のNビット10コード数の最上位ビットは“0”である。同様に、我々が、

次の存在する最も低い万能コードが番号“7”であることを見つけ、それが“1”であることが分かった場合、我々の次の最上位ビットは“1”である。適切に行くと、このシステムは、印刷紙在庫シリアル番号を、ある登録または印刷紙自体の製造業者に登録している限り、著作権所有者まで明確に追跡することができる。すなわち、我々は、万能理め込みコード47、11、12、15、19、21、26、27、28、34、35、37、38、40、および48を使用し、埋め込みコード0110 0101 0111 0100を有する印刷紙が、カナダ在住の未知の野性動物写真家兼、本明映画監製師であるLeonard de Bottilierの所有物であるという登録を調べる。彼が無視で登録した彼のフィルムおよび印刷紙の在庫を、彼がこの在庫を購入したとき、馬鹿げた簡単なプロセスを行う“郵便の必要がない”製造会社が親切にも準備した封筒に入れる。数秒の仕事のため、我々はこれを知っている。Leonardに著作権使用料を支払う必要がある誰かが、それが現れることをチェックし、確実に登録は、著作権使用料の支払いプロセスをそのサービスの一部として自動化する。

[0173]

ある終点は、真に洗練された著作権侵害者と、違法の目的を持った他の者とは、種々の暗号化方法を実際に使用してこれらの万能コードを解読することができ、これらを販売し、コードを除去または歪ませるのを助けることができるソフトウェアおよびハードウェアツールを制作することである。しかしながら我々は、これらの方法を、本明組書の一部として教えない。とにかく、これは、万能コードの容易さとこれらが聞く用途に支払う必要がある値段の1つである。

[0174]

万能コード：2）決定論的公式を基礎とする万能コード

万能コードのライブラリは、万能コードを付けられている信号および画像の存在および身元を聞く鍵としての数メガバイトの独立した一般的にランダムなデータを記憶および交換することを必要とする。代わりに、種々の決定論的公式を、ランダムデータ/画像フレームの発生に使用し、これらによって、これらのコードのすべてをメモリ内に記憶することと、“50個”の万能コードの各々に質問することとを回遊することができる。決定論的公式は、所定の信号または画像中に存在することが一度知られている1Dコードを決定する処理を高速化することを助けることもできる。他方では、決定論的公式を、あまり洗練されていない著作権侵害者によって追跡することができる。一度追跡されると、これらを、インターネット上で100個のニュースグループに提示するように、より簡単に伝達することができる。これらは、追跡および公表をかわない多くの用途には適切であり、独立万能理め込みコードを発生する決定論的公式を、単にチケットとすることができる。

[0175]

万能コード：3）“簡単な”万能コード

この分類は、はじめの2つを結合したものの一部であり、この技術の原理の真に大きな規模の実施に最大限向けたものである。この機能を使用する用途は、信頼できる安全性が、低費用で大きな規模の実施と、これが可能にする莫大な経済的利益とほとんど重要ではない形式のものである。一例としての用途は、検証認識ユニットを適度に値付けされた（レレジョンのような）家庭用オーディオおよびビデオ装置中に直接配置する。このような認識ユニットは、代表的に、オーディオおよび/またはビデオを監視してこれらの著作権検証コードを探し、そこから、記録可能性が与えられているか否か、または中央オーディオ/ビデオサービス提供者に伝送されるとともに毎月の送り状に配置される番組特定データベースの増加のような判断に基づいて簡単な決定を行う。さらに、バーおよび他の公共の場所における“フックボックス”が、著作権を持った題材を監視し（マイクロフォンによって聞き）、ASCAP、BMI、等によって使用される詳細な報告書を生産することができる。

[0176]

簡単な万能コードの中心となる原理は、いくつかの基本的な業界標準の“ノイズ状”で繰り返しのない繰り返しのパターンを、信号、画像、および画像列中に挿入し、安価な認識

ユニットが、A) 著作権“フラグ”の存在を決定するか、B) Aに追加して、より複雑な決定処理および動作を容易にすることができるようになることである。

[0177]

本発明のこの実施例を実現するために、独立理め込みノイズ信号を発生する基本的な原理を、安価な認識信号処理ユニットに適用させると同時に、有効なランダム性およびホログラフィックの透過性性質を維持するために、簡単にする必要がある。これらの簡単なコードの大規模産業への採用によって、コード自体は公衆情報と隣接し（ケーブルスクランプリングボックスがほとんど事実上の公衆であるように）、フラッグマーケット対策を開発するために限定された著作権侵害者に対してドアを開いたままであるが、この状況は、ケーブルビデオのスクランブル化や、このような違法活動の客観的・継続的分析とまったく類似している。

[0178]

順向の著作権検出のこの一般的な領域における本出願人に既知のある先行技術は、オーディオ業界における多くの会社によって採用されたシリアルコピー管理システムである。本出願人の知っている限り、このシステムは、オーディオデータストリームの一部ではないが、それにもかかわらずオーディオストリームに挿入され、関連するオーディオデータを検索すべきか否かを示すことができる。非オーディオ“フラグ”信号を使用する。このシステムが有する1つの問題は、この追加の“フラグ”信号をサポートすることができる媒体および装置が制限されることである。他の欠陥は、フラグシステムが、より複雑な決定を行うのに使用できる身元情報を搬送しないことである。さらに他の困難は、アナログ信号の高品質なオーディオ標準化が、あるデジタルマスタの完全なデジタルコピーを任意に近く行えるようになる恐れがあり、この可能性を禁じる対策は、無いように思われる。

[0179]

本発明の原理を、オーディオ用途、ビデオ、および上述した他のすべての用途における、これらおよび他の問題を影響を与えることができる。簡単な万能コードの用途の一例は、以下のようなものである。ある1つの業界標準“1. 0 0 0 0 0 0 0 0のノイズ”は、なんらかの所定のオーディオ信号の著作権符号の存在または不在を示す最も基本的なものとして規定される。図9は、業界標準ノイズ秒が時間領域4 0 0および周波数領域4 0 2の双方においてどのように見えるかの一例である。定義によって、連続整数であり、標準化レートおよびビット量子化の何らかの組み合わせに適合する。規格化された振幅を有し、どのようなデジタル信号帯域にも任意に尺度合わせることができる。この信号の信号レベルおよび最初の10番目の増幅数は、2つの境界4 0 4において連続であり（図9 C）、その結果、繰り返し場合、信号における“不連続”は（波形として）目に見えない、または、ハイエンドオーディオシステムによって検出される場合、聞き取れない。1秒の選択は、この例において任意であり、この間隔の正確な長さや、可能性、擬似ホワイトノイズ特徴、書き目のない繰り返し可能性、認識処理の容易さ、および著作権を付ける決定を行えることによる速度的な理由から得る。この繰り返しノイズ信号の信号または振幅への（再び、人間の知覚力以下のレベルにおける）挿入は、著作権材料の存在を示す。これは、本質的に1ビット検証コードであり、他の検証技術の埋め込みを、この点において後に論ずる。この検証技術の使用を、ここで論ずる低価格家庭向け器具を適に導入に拡張することができ、スタジオにこの技術を使用することができ、監視局を設定し、実際に数1 0 0チャンネルの情報を同時に監視し、マークされた信号ストリームを探索し。さらに、課金ネットワークおよび印刷追跡システムに適合する関連する身元コードを探索することができる。この基本的な標準化ノイズ署名を、書き目無く何度も繰り返し、基本著作権検証をマークすべきオーディオ信号に加える。“簡単”という言葉の理由の一部は、以下のように理解される。明らかに著作権侵害者は、この業界標準信号について知るであろうが、削除または改ざんのようなこの知識から得られる彼らの違法な使用は、大規模な市場に対する全体的な技術の経済的な価値に比較して、経済的に非常に小さいものとなる。大部分のハイエンドオーディオに関して、この信号を、フルスケールから8 0から1

0 0 4 dB 低下またはさらに小さいものとし、各々の状況を、たとえ推測されるものが確実に存在しても、それら自身のレベルに選択することができる。信号の種類を、ノイズ署名が用いられているオーディオ信号レベルに低くて変調することである。すなわちこの振幅を、ドラムビートの場合、意味のある程度、しかし聞き取れるまたは不慣れなるほど制約ではない程度に増加することができる。これらの程度は、記述すべき認識回路網を単に助ける。

【0180】

このノイズ信号の存在の低確率な機器による誤読を、種々の方法において行うことができる。あるものは、オーディオ信号出力の測定 of 簡単な原理に対する基本的な変形に基づいている。ソフトウェア認識プログラムを書くことができ、さらに選択された数字の検出アルゴリズムを、より高い信頼性のある検出を行うために用いることもできる。このような実施例において、著作権ノイズ署名の検出は、オーディオ信号の時間平均された出力レベルと、ノイズ署名を減算した同じオーディオ信号の時間平均された出力レベルとの比較を含む。ノイズ信号を減算されたオーディオ信号が、変更されていないオーディオ信号より低い出力レベルを有する場合、著作権署名が存在し、同じ意味で、ある状態フラグを設定する必要がある。この比較の実行において含まれる主眼的に検知するものは、オーディオの録音再生速度が不一致（例えば、ある機器は、正確に1秒情報に関して0.5% “遅い” かもしれない）である原理と、何らかの所定のオーディオ中の一秒のノイズ署名の未知の位相の処理（基本的に、この“位相”は、0から1秒位までもかもしれない）を含む。上述した2つほど中心的なものではないがそれにもかかわらず説明すべき他の検知するものは、認識回路が、オーディオ信号に元々埋め込まれたノイズ署名より大きい振幅のノイズ署名を減算すべきではないことである。幸運にも、これを、単に小さい振幅のノイズ信号のみを減算することによって実行することができ、出力レベルが低下した場合、これは、出力レベルにおける“谷に向かっている”しるとなる。さらに他の関連する検知するものは、出力レベルの変化が、全体の出力レベルに対して極めて小さく、計算を一般に適切なビット精度によって、例えば、時間平均された出力レベルにおいて16〜20ビットオーディオにおいて、32ビット値演算および集積によって行う必要があることである。

【0181】

明らかに、低確率用用途のこの出力レベル比較処理回路を設計し組み立てることは、技術的最適化の仕事である。ある交換は、より低い価格と複雑さのために回路網に形成することができる“近道”に関する検証の実行における精度である。この認識回路網の機器内の配置の好適実施例は、その仕事用に注文生産した1つのプログラム可能集積回路によるものである。図10は、あるこのような集積回路506を示す。ここで、オーディオ信号が、デジタル信号として、または1C500内でデジタル化すべきアナログ信号として500中に入り、出力信号は、著作権ノイズ署名が見つかった場合にあるレベルに設定され、見つからなかった場合に他のレベルに設定されるフラグ502である。標準化ノイズ署名波形を、1C506内の読み出し専用メモリ504に記憶することも示す。オーディオ信号の1C506への適用と、有効なフラグ502の出力との間には、認識を行える前に、オーディオのある有限の位置を監視する必要があるため、僅かの時間遅延が存在する。この場合において、著作権ノイズ署名の存在または不在の正確な実行のために十分な時間を有する場合、1Cが外界に知らせる“フラグ有効”出力信号が必要になるかもしれない。

【0182】

図10の1C506の基本的な機能を実行するのに用いられる特定の設計および設計の哲学の広い範囲の変形例が存在する。オーディオ技術者およびデジタル信号処理技術者は、いくつかの基本的な異なる設計を生産することができる。あるこのような設計を図11において、それ自体は、後に論議するような他の技術的最適化に基ずく集積回路509によって示す。図11は、アナログ信号処理ネットワーク、デジタル信号処理ネットワーク、またはソフトウェアプログラムのプログラミングステップのいずれかのフローチャー

トを示す。我々は、ある経路に沿った入力信号600を、時間平均パワーメータ602に供給し、結果として得られるパワー出力を直接、信号 P_{avg} として扱うことに気づく。右に示して、我々は、604で通常速度の125%において読み取られ、したがってそのビッチが変化した、606で“ビッチ変換ノイズ信号”を示す。標準ノイズ算を504を見つける。次に、ステップ608において入力信号からこのビッチ変換ノイズ信号を減算し、この新たな信号を、602において示したのと同じ形式のここでは610で示す時間平均パワーメータに供給する。この操作の出力信号も、ここでは610で P_{avg} と示す時間基準信号である。次にステップ612でパワー信号610からパワー信号602を減算し、パワー差信号 P_{diff} 613を生じる。万能標準ノイズ署名が、入力オーディオ信号600において実際に存在する場合、ケース2、618が、発生し、4秒間程度のビート信号が、出力信号613において現れ、図12、622のようなステップによってこのビート信号を検出しなければならない。ケース1、614は、周期的なビートが見られない一般的なノイズ信号である。ステップ604における125%を、ここでは任意に選択しており、技術的な理由が最適値を決定し、異なるビート信号間隔数618を導く。この例における4秒の持続は、事実上一定期間であるが、極く少なくとも2つまたは3つのビートを検出したい場合、図12は、図11の基本設計を、隔から0.05秒遅延させたオーディオの部分において各々一斉に動作する20個の並列回路によって1/20秒程度遅延させた入力信号の種々の遅延されたバージョンにどのように繰り返し使用されるかの概要である。この方法において、ビート信号が、1/5秒程度毎に見られ、ビート検出回路の列を下る進行波のように見える。この進行ビート波の存在または不在は、検出フラグ502をトリガする。同時に、例えば、少なくとも2秒のオーディオが、フラグ有効信号508を設定する前に閉じられることを保証するオーディオ信号モニタが存在する。

【0183】

オーディオの例を記述してきたが、ある繰り返し万能ノイズ信号または画像の同様の形式の定義を、多くの他の信号、画像、写真、およびすでに論及した物理的媒体に用いることができることは、当業者には明白であらう。

【0184】

上述したケースは、情報の1ビット面のみを取り扱った、すなわち、ノイズ署名信号を、存在するか(1)、しないか(0)とした。多くの用途に関して、さらに複雑な判定か、または課金明細書におけるログ情報等に使用することができるシリアル番号情報をさらに検出することが好ましい。上述したのと同様の原理を用いるが、ここでは、図9に示すようなN個の独立ノイズ署名が、1つのこのような署名の代わりに存在する。代表的に、あるこのような署名は、これによって著作権マーキングが単に存在することを検出するマスタとし、これは一般に他のものより大きいパワーを有し、次に他のより小さいパワーの“検証”ノイズ署名をオーディオに埋め込む。認証回路は、一度主要なノイズ署名の存在を見つけたら、他のN個のノイズ署名に進み、上述したのと同様のステップを用いる。ビート信号が検出される場合、これは1のビット値を示し、ビート信号が検出されない場合、これは0のビット値を示す。代表的にNを32とし、2³²個の検証コードを、本発明を使用する何らかの所定の産業に対して利用できるようにすることができる。

【0185】

検証コードの長さがある場合のこの技術の使用

本発明の原理を、1つの検証信号——もし望むなら指紋——の存在または不在のみを使用し、ある信号または画像が著作権を与えられていることの信頼性を与える場合において、明らかに適用することができる。業界標準ノイズ署名の上述した例は、ある適切な場合である。我々は、もはやコイン投げとの類似性の追加の信頼性を持たず、我々は、もはや追跡コード容量または基本シリアル番号容量を持たないが、多くの用途は、これらの属性を必要としないであろうし、1つの指紋による追加の簡便さは、なんらかの事象におけるこれらの他の属性を捨てて余りある。

【0186】

“指紋”との類似性

“ホログラフィック”という言葉を、本明細書において、どのように検証コード番号を大部分が完全な形態において符号化信号または画像全体に分散させるかを記述するのに使用してきた。これを、信号または画像の何らかの所定の断片は、完全な固有検証コード番号を含むという概念にも適用する。ホログラフィの物理的な実施の場合、この特性を失い始める前に、断片をどの位小さくできるかにおいて制限があり、ここでホログラフィック媒体の分解能制限は、ホログラム自体に関する主要な要素である。図4の符号化装置を使用し、ゼロがランダムに1または-1に変化する上述した我々の“設計されたノイズ”をさらに使用する非改変配布信号の場合において、必要な断片の密度は、信号または画像のスタラインにおいて単にN個の連続的な標本であり、ここでNを、予め規定した我々の検証コード番号の長さであるとする。これは、情報の量であり、すなわち、ノイズおよび改ざんが作用する実期的な状況は、一般にこの簡単な数Nより1、2、またはは1以上大きい所の標本を必要とする。当業者は、これによって検証を行うことができる最も小さい断片の寸法における正確な統計の明確な定義に含まれる多くの変形が存在することを認識するであろう。

[0187]

教授の目的のために、本出願人は、固有検証コード番号を、画像（または信号）を横切って“壁紙貼りした”というアナログも使用する。すなわち、画像全体に何度も繰り返す。IDコード番号のこの繰り返しを、図4のエンコーダの使用におけるように定期的にすることができ、またはそれ自身ランダムにすることができ、図6のIDコード216のビットは、通常の繰り返し方法において停止せず、各々の標本においてランダムに選択され、このランダムな選択は、出力信号228の値とともに記憶される。とにかく、IDコードの情報キャリア、独立型の込みコード信号は、画像または信号を横切って変化する。したがって、壁紙との類似性を要約すると、IDコード自体を何度も繰り返すが、各々の繰り返しがつけるパターンは、一般に追跡できない環に従って、ランダムに変化する。

[0188]

損失データ圧縮

上述したように、好適実施例の検証符号化は、損失データ圧縮およびその他の伸長とに附えうる。このような圧縮は、特にデジタル化された娯楽番組（映画、等）のような状況における使用が益々増えると思われる。

[0189]

本発明の好適実施例によって符号化されたデータは、出願人に既知のすべての形式の損失圧縮に耐えうるが、商業的に最も重要だと思われるものは、CCITT G3、CCITT G4、JPEG、MPEGおよびJBIG圧縮／伸長標準である。CCITT標準は、黒および白の文書の圧縮（例えば、ファクシミリおよび文書記録）において広く使用されている。JPEGは、静止画に最も広く使用されている。MPEGは、動画に最も広く使用されている。JBIGは、黒および白の像への使用に関して、CCITT標準の有望な後継者である。これらのような技術は、損失データ圧縮の分野において良く知られており、良い概略を、Pennebaker et al., JP6, Still Image Data Compression Standard, Van Nostrand Reinhold, N.Y., 1993において見ることができる。

[0190]

ステガノグラフィおよび、より複雑なメッセージまたは情報の伝送におけるこの技術の使用

本明細書は、信号全体に1つの検証コードの壁紙貼りと同記において呼んだものに集中する。これは、多くの用途に関して所望の精度であると思われる。しかしながら、メッセージを通過させる、または適切な検証情報の極めて長い列を信号または画像中に埋め込むことが望ましい他の用途が存在する。多くのこれらの考えられる用途の1つは、所定の信号または画像がいくつかの異なるグループによって操作されることを意図され、画像の特定の領域が、各々のグループの適切な操作情報の検証および挿入に確保されている場合である。

[0191]

これらの場合において、図6におけるコードワード216を、ある予め決められた方法において、信号または情報位置の関数として実際に変化させることができる。例えば、画像において、コードをデジタル画像の各々すべてのピクセルラインに順次して変更することができる。16ビットコードワードを216とすることができ、各々の走査ラインは新たなコードワードを有し、したがって480の走査ライン画像は980バイト(480×2バイト)メッセージを通過させることができる。メッセージの受信者は、メモリ214に記憶されたノイズ信号にアクセスするか、使用されている符号化方法のノイズコードの万能コード構造を知る必要がある。本出願人の知る限り、これは、ステガノグラフィの成熟した領域の新規のアプローチである。

[0192]

万能コードの前述の3つの用途のすべてにおいて、万能コードに加えて、短い(ひとつとすると8または16ビット)秘密コードを追加することがしばしば望まれる。これは、洗練された著作権侵害者による万能コードの削除の可能性に対する他の僅かな量の安全性をユーザにたもたす。

[0193]

本人の先行出願

この点に対する詳細な説明は、PCT国際公開パンフレットWO95/14289号として公開されている本願人の先行国際出願の開示を単に繰り返した、上記単なる繰り返し、以下の開示に対する背景を与える。

[0194]

N側の独立した埋め込みコード信号からの区別としての1つのマスタコード信号

ひとつとするとリアルタイムエンコーディング部分において例示されるこの開示のある部分において、N側の独立したソース信号同一空間埋め込み信号を、なにも所定の埋め込みコード信号の非ゼロ要素がその埋め込みコード信号に対して固有になるように設計する節約ステップを行った。より慎重に、所定の信号のある画素/標本点を、我々のNビット識別ワードにおけるある予め決められたm番目のビット位置に“割り当てる”。さらに、かつ実装化の他の基本的な最適化として、すべてのNの埋め込みコード信号に渡るこれらの割り当てられた画素/標本の集合は、正確に前記ソース信号の範囲であり、ソース信号における各々のそしてすべての画素/標本位置が、我々のNビット識別ワードにおける唯一のm番目のビット位置に割り当てられることを意味する。(しかしながら、各々のそしてすべての画素を変更しなければならないとは言えない。)単純化のため、我々は次に、Nの独立した信号よりも、1つのマスタコード信号(または“零埋め込み”)について述べることができ、このマスタ信号における予め規定された位置が我々のNビット識別ワードにおける固有ビット位置に対応することを実現する。したがって我々は、この回り道を越えて、信号マスタノイズ信号におけるこのある程度高度な概念を構成する。単なる節約および単純化を越えて、我々のNビット識別ワードにおける複数のビット位置が、もはや1つの画素/標本の情報伝送容量に対して“十分”でないという考えから元々は得られた、この移動に関する性能的理由も存在する。

[0195]

この1つのマスタをより明確に理解することによって、我々は、この開示の他の部分を新たに見出すことができ、与えられた用途領域内での更なる詳細を探究することができる。

[0196]

マスタコード概念を使用する大部分の決定論的万能コード

適切な1つの場合は、万能コードに対する部分において項目“2”と呼ばれる、決定論的万能コードの使用をさらに探究することである。この技術の所定のユーザは、この技術の原理の以下の種々の使用を選択することができる。当のユーザを、ホームビデオの大手配給者としてもよいが、明らかに、前記原理は、この技術のすべての他の潜在的ユーザに広がる。図13は、含まれるステップを模式的に示す。この例において、ユーザを“エイリアンアポカリプシス”とする、彼等は最初に、彼等の映画“ババの冒険”のビデオフレームの手法と同一の空間に広がる画像キャンバスを形成する。このキャンバスにおいて

、彼等は前記映画の名前を印刷し、彼等のロゴおよび社名を配置する。さらに、彼等は、彼等が現在作りだしている大量の複製に対する分配ロットのような特別な情報を下部に有し、示したように、彼等は実際に、示された固有フレーム数を有する。したがって、我々は、オリジナルの映画フレームに付加され、出力配布可能フレームを形成するマスタ雪状画像（マスタコード信号）の形成の初期の基礎を形成する標準画値700の例を見つける。この画値700を、白黒またはカラーのいずれとしてもよい、この画値700を縦横ランダムマスタコード信号に変換する過程は、前記暗号化/スクランブル化ルーチン702によって言及され、ここで、オリジナルの画値700は、なんらかの多数の既知のスクランブル化方法を受け、番号“28”の記法は、実際にスクランブル化方法のライブラリとすることができると観念に言及し、この特定の映画、またはこの特定のフレームに使用される個々の方法を変更することができる。その結果、我々の古典的なマスタコード信号または雪状画像となる。一般に、その確度値は高く、空きチャネルに切り替えたテレビジョン受信機において極めてよく前記雪状画像が見えるが、明らかに、有益な画値700から得られ、スクランブル化702を通じて変換される。（注意：この例の画値の巧み方は、実際にある程度下手な偽装であり、本発明者を利用してできる粗末な道具の機能である）。

【0197】

次にこのマスタ雪状画値704を、本開示の他の部分において暗号を述べた我々のNビット識別ワードによって変調された信号とし、結果として得られる変調信号を、確度において、許容しうる知覚されるノイズレベルに低下させ、前記オリジナルフレームに付加し、配布可能フレームを発生する。

【0198】

図13に示す方法がもたらす種々の利点および特徴が存在する。この変形全体において種々のテーマも存在する。明らかに、1つの利点は、ユーザが、彼等の仕事に押印し、署名するために、より直接的に個人化した方法を使用できることである。暗号化/スクランブル化ルーチン702を、高いセキュリティのものとして共に公開せず、翻改しないとする。著作権従事者達がロゴ画値700の知識を有しているとしても、この知識をマスタ雪状画値704を造跡することができるようにするために使用することができず、したがって、いかなる、本システムを解説することはできない。他方において、簡単な暗号化ルーチンは、本システムを解説するドアを開くことができる。図13の方法の他の明らかな利点は、他の情報を防御アクセス全体に配置する能力である。正確に言うところ、ロゴ画値700に含まれる情報を、前記最終的な配布可能フレームにおいて直接輸送しない。すなわち、暗号化/スクランブル化ルーチン702が、ビット切断エラーを許容する簡単な既知の暗号解読/デスクランブル化方法を有する場合、一般に、配布可能フレームと、Nビット識別コードワードと、使用された確度低下係数と、使用すべき暗号解読ルーチンの数とを有することを基礎として、画値700を完全に再形成することができる。画値700の正確な再形成が可能ない理由は、前記低下動作それ自体と、相伴うビット切断とのためである。しかしながら、現在の論考に関して、この問題全体は、いくぶんアカデミックである。

【0199】

図13のテーマにおける変形は、実際にNビット識別コードをロゴ画値700に直接配置することである。ある意味において、これは自己参照となる。したがって、我々が、我々の保管するロゴ画値700を取り出す場合、我々の識別ワードがすでに含まれ、我々は暗号化ルーチン#28をこの画値に用い、スケルトンし、このバージョンを使用し、この開示の技術を使用して疑わしい画値を復号化する。このようにして見つかったNビットワードは、我々のロゴ画値700に含まれるものと一致する。

【0200】

暗号化/スクランブル化ルーチン702の1つの望ましい特徴を、フレーム番号の1つの数字変化のような小さい変化を入り画値700にもたせた場合、出力スクランブル化マスタ雪状画値704において大きな確度的変化が存在するようになることとしてもよい。さらに、実際のスクランブル化ルーチンは、フレーム番号の関数として変化してもよく、疑

乱ランダム化機能において代表的に使用されるある“シード”数が、フレーム番号の関数として変化することができ、したがって、高いレベルのセキュリティを保持するのを助けるための実形例の方法が可能である。結局、工学的な最適化の考察が、これらのランダム化方法のいくつかの間で関係と、これらが、非圧縮ビデオストリームを、MPEG圧縮方法論によるように、圧縮ビデオストリームに変換する過程を通じて許容しうる信号強度レベルを保持することにどのように関係するかを研究することを開始するであろう。

【0301】

符号化過程702の他の望ましい特徴は、情報的に効率的である、すなわち、どのようなランダムな入力を与えた場合も、純然たるランダムさを越える残留空間的パターンがわずかなであるかまったくない本質的に空間的に一様なノイズ面値を出力できるべきであることである。どのような残留空間パターンも、Nビット識別ワードの符号化の非暗号化と、他の道具を著作権侵害志望者に公開し、本システムを破壊することに寄与する。

【0302】

図13の方法の他の特徴は、復号化システムの部分としての識別できる記号の使用に対するより直観的なアピールであり、これは、法廷の本質的に一般の環境において有利に解釈すべきである。それは、どこかに言及されているコイン投打器固有の単純化される。陪審員または裁判官は、疑わしいコピーを盗まれているとして認識する鍵の1つとしてオナのロコをよりよく示すであろう。

【0303】

厳密に言って、ロコ画値700はランダム化するためには必要ないことも言及すべきである。前記ステップを、ロコ画値700に直接用いることができる。本発明者には、何が実際的なゴールなのかまったく明らかでない。N=1の場合に対するこの概念のささいな拡張は、単純かつ容易に、ロコ画値700を単にオリジナル画値に極めて低い難度レベルにおいて付加する場合である。本発明者は、すべての新規事項においてあるべきこのささいなケースを推定しない。多くの点において、これは、サブミナル広告の音からの問題と同様であり、画値に付加された低光レベルパターンは、人間の眼/脳システムに認識可能であり、恐らく、人間の脳において、無意識レベルにおいて動作する。現在の技術のこれらのささいな拡張を指摘することによって、うまくいけば、このような既知の先行技術に関して本発明の新規の原理を識別することをさらに明らかにすることができ。

【0304】

5ビット縮小英数字コードセットおよび他

Nビット識別ワードに関する幾つかの用途において、名前、会社、ストレンジワード、メッセージ等を実際に表すことが望ましい。この開示の大部分は、Nビット識別ワードを、単に、高い統計上のセキュリティと、インデックス化トラッキングコードと、他のインデックスを基礎とするメッセージ伝送とに使用することに焦点を合わせている。彼らおよびオーディオ内の“不可視署名”の情報伝送容量は、いくらか制限されているが、我々が実際に英数字項目をNビット識別ワードに“書き込む”場合、我々のNビットを効率的に使用することが賢明である。

【0305】

これを行うための1つの方法は、英数字メッセージを通過させる減少ビット（例えば、8ビットアスキーより少ない）標準化コードを規定、または、既に存在するものを使用することである。これは、いくつかの用途の一部におけるこの必要性を満たすことを助けることができる。例えば、簡単な英数字コードを、例えば、文字V、X、QおよびZを含まないが、数字0ないし9を含む5ビットインデックステーブルにおいて構成することができる。この方法において、1000ビット識別ワードは、20の英数字記号と共に伝送することができる。他の選択肢は、より難解に使用される記号がより短いビット長コードを有し、あまり難解に使用されない記号がより長いビット長を有する。テキスト圧縮ルーチンにおいて使用されるもののような可変ビット長コードを使用することである。

【0306】

疑わしい信号におけるNビット識別ワードを検出し、認識することにおける追加

古典的に言えば、Nビット識別信号の検出は、ノイズにおける既知の信号を検出する古い技術によく適合する。この上の上におけるノイズを、極めて広く解釈することができる。下にある署名信号を検出する必要がある。画像またはオーディオトラックを自己体をノイズと考えることができる。このより古い技術に対する多くの参考文献の内の1つは、カッサム、サレーム、エーの本、"非正規ノイズにおける信号検出"スプリングカーハウス、1988(よく前記された図書館において一般に利用可能であり、例えば、国会のユー、エス、図書館においてカタログ番号75102.5、K357 1988 によって利用できる)である。本発明者の現在の理解の限り、この本における題材を、出願人の埋め込み信号の特性を発見する問題に直接適用できないが、より広い原理を適用できる。

[0037]

特に、カッサムの本の1、2章"仮説検定の基本概念"は、真"1"をある仮説とし、値"0"を他の仮説とすると、バイナリ仮説の基本概念を広げる。この章の最後の段落は、上述した実施形態、すなわち、"0"仮説が"ノイズのみ"の場合に対応し、"1"が観測における信号の存在に対応する場合に関する点にある。しかしながら、真の極性の出願人の使用はこれと同じではなく、ここでは、"0"は"ノイズのみ"よりも反転信号の存在に対応する。本実施形態においても、"ノイズのみ"の場合を実際に無視し、識別過程が、我々のNビット識別ワードを与えるか、"ゴミ"を与える。

[0038]

埋め込みコード信号の検出における継続し、必然的な工業的効果は、既知の信号検出のこの豊かな分岐から、確実に多量に適用するであろう。この分岐において普通の良く知られた技術は、いわゆる"適応フィルタ"であり、これは、カッサム本の2章において付随的に説明されている。信号処理における多くの基本的な教科書は、信号検出の方法における論考を含んでいる。これは、いくつかの分野において相関検出として既知である。さらに、既知の信号の位相または位置が、しばしばこの技術の用途における場合のように、先天的に既知である場合、適応フィルタを、しばしば、疑わしい画像と我々のNビット識別ワードにおけるm番目のビットプレーンに関連する埋め込み信号との間の簡単なベクトルドット積に減少させることができる。これは、疑わしい画像を取り上げ、その列が予め埋め込まれたNビット識別ワードに対応するかどうかを決定する目的を有する1および0のシーケンスを発生する。さらに他の簡単な"検出アルゴリズム"を表す。例えば、図3を参照すると、我々は、これらのプロセスステップを進み、オリジナル画像を疑わしい画像から減算することを含み、次のステップは、単に、すべてのNのランダム独立信号を込むことであり、これらの信号と差信号との単純なベクトルドット積を計算しそのドット積が負の場合、"0"を割り当て、そのドット積が正の場合、"1"を割り当てる。この"多くのうちの1つ"のアルゴリズムの慎重な分析は伝統的な適応フィルタとの類似性を示すであろう。

[0039]

極めて低いレベルの埋め込みコード信号を正確に検出する増加した能力を与えることができる。"適応フィルタ"および"相関形式"に対する幾つかの直接的な改善も存在する。これらの改善のいくつかは、前記カッサム本において説明された原理から得られ、他のものは、本発明者によって発生され、本発明者は、他の論文または仕事においてこれらが現れるかについての知識を持たず、進歩した信号検出技術に対する完全な広範な調査も行っていない。あるこのような技術は、カッサム本の7ページの図3、5によって再示されるものがひとつとすると最適であり、検出のための一般的なドット積アルゴリズムアプローチに用いることができる種々の局所的最適化重み付け係数のいくらかのプロットが存在する。すなわち、単純なドット積を計算するよりも、全体のドット積における各々の要素の乗算を、差信号それ自体に、すなわち、低レベルの既知の信号が埋め込まれている中の信号についての既知の先天的統計情報を基礎として重み付けすることができる。これらの結果にまだ精通していない興味を持った読みに、カッサムの3章を読み、より完全な理解を得ることを勧める。

[0040]

カッパムの本において明白に存在するように見え、本発明者によって基礎的に開発された原理は、全体として、疑わしい信号の統計的特性の大きさに対する、押している既知の信号の統計的特性の大きさの利用を含む。特に、問題の場合には、我々が推定している埋め込まれた信号が、差信号において存在するノイズおよび改ざんよりもかなり低いレベルである場合であるように思われる。図1-14は、このアプローチに続く推論に対するステージの設定を試みる。上部の図720は、代表的な“問題の”差信号、すなわち、その中に存在するかもしれず、存在しないかもしれない埋め込まれた信号よりもかなり高い全体的なエネルギーを有する差信号のヒストグラムにおける差における一般的な様子を含む。“平均を除去した”という言葉は、単に、差信号および埋め込まれた信号の双方の平均が、規格化ドット積を行う前の一般的な定義によって除去されていることを意味する。次に、下部の図722は、これら2つの信号の周波数、または直線の場合においてスケール勾配の一般的な同様のヒストグラムプロットを有する。純粋な検査から、周波数変換領域における簡単なしきい値化演算と、その後の信号領域への逆変換とは、いくつかのバググラフのドット積“識別アルゴリズム”における程度の先天的なバイアスを取り除くことに向かう長い道を行くことになる。ここで、しきい値化は、差信号周波数値の絶対値があるしきい値を越える場合、そのしきい値を単に置き換えるというアイデアのことを呼ぶ。このしきい値を、埋め込まれた信号のヒストグラムを最大に含むように選択することができる。

[0211]

ドット積アルゴリズムにおけるバイアス効果のいくつかを“軽減”することにおける重要な援助とすることができる他の演算は、差信号における低次周波数の除去であり、すなわち、差信号をハイパスフィルタに通すことであり、ここで、ハイパスフィルタに関するカットオフ周波数を、元の(またはDC)周波数に比較的近くなる。

[0212]

圧縮され、伸張された信号における埋め込み信号を認識するか、非一様エラー源を形成するある既知のプロセスを受けたなんらかの信号内の埋め込み信号を認識する特別な考察

基本概念に関する長いタイトル。画像/ビデオ圧縮のJPEG/MPEGフォーマットによる画像の圧縮および伸張のような、いくつかの信号処理動作は、ある相関および構造を有するある一定の変換領域においてエラーを形成する。例としてJPEGを使用すると、所定の画像をいくらか高い圧縮比で圧縮し、伸張し、結果としての画像をフーリエ変換し、オリジナルの非圧縮画像のフーリエ変換と比較すると、一定のパターンが明白に可視になる。このパターン化は、相関エラー、すなわち、ある程度量化でき、予測できるエラーのしるしである。この相関エラーのより高い特性の予測を、JPEG圧縮が、これらの見てすぐと分かるエラー署名を残す他の動作を受けたからとれないある面白い画像内の埋め込みドットコード信号を認識することによって論じた方法において有利に使用することができる。基本的なアイデアは、既知のより高いレベルのエラーが存在する領域において、前記認識方法のほかに、既知のより低いレベルの相関エラーを有する領域に対して小さくすることである。しばしば、エラーの予測されるレベルを量化し、この量化を再変換された信号値を適切に重み付けすることに使用することができる。再び例としてJPEG圧縮を使用すると、疑わしい信号をフーリエ変換することができ、フーリエ空間表現が、見てそれと分かる箱格子パターンを明らかに示すことができる。次にフーリエ空間信号を、格子点付近で“空間フィルタ処理”することができ、次にこのフィルタ処理化表現を、その通常の時間または空間領域に変換し戻し、次に本開示において与えられた認識方法を行うことができる。同様に、非一様エラー源を形成するなんらかの信号処理方法を、これらのエラー源が非一様となる領域に変換することができ、これらのエラー源の高い点における値を減少させることができ、このように“フィルタ処理された”信号を、標準的な認識のための時間/空間領域に変換し戻すことができる。しばしば、この全体のプロセスは、適切なフィルタ処理プロファイルで“設計”するために、代表的な相関エラーの動作を“特徴化”する長く困難なステップを含むであろう。

[0213]

“署名コード”および“不可視署名”。

簡単に、かつ明確にするために、“署名”、“不可視署名”および“署名コード”という言葉を、科学技術の一般的な技術を示し、しほしは、特に本開示において前に規定した概念の含みコード信号を示すために使用し、使用し続ける。

【0214】

動画への署名コードの組み込みにおける更なる仕組み

静止画を圧縮するJPEG標準と、動画を圧縮するMPEG標準との間にあるため、不可視署名を静止画に配置すること、署名を動画に配置することの間に差がある。JPEG/MPEG差によるように、異なる基礎の問題ではなく、動画によって、パラメータとして時間を含むことによって、工業的最適化の新たな次元が開くことである。MPEGに関連する多くの数値も、どのようにMPEGが（一般に）単にJPEGをフレームずつを基礎として用いていないかについての部分を必ず含むであろう。この技術の原理の用途と同じく、一般的に言って、動画シーケンスへの不可視署名の配置は、単に別々に不可視署名をフレーム毎に配置することではない。動画知識の精神的物理学にいくらか関係する種々の時間を基礎とする理由が作用し、他は、単純な費用工学的理由によるものである。

【0215】

ある実施形態は、実際に、MPEG圧縮標準を解決法の1つとして使用する。すでに発明されているか、まだ発明されていない他の動画圧縮方法を、等しく良好に使用することができる。本例は、図13に示し、本開示において論考したマスタ雪状画像の発生のために、スクランブル化ロゴ画像アプローチも使用する。

【0216】

“圧縮マスタ雪状画像”を、図15に示すように別個にレンタリングする。“レンタリング”は、ビデオ、映画およびアニメーション制作において一般に熟知の技術を示し、これによって、画像または画像のシーケンスを、コンピュータ命令のような構成的技術か、手によるアニメーションセルの描画によって形成する。したがって、本例における署名映画を“レンタリングする”ことは、本質的に、デジタルファイルとしてコンピュータ形成しようとするとか、それを形成するあるカスタムデジタル電子回路網を設計することである。

【0217】

図15において概要を示した手順の全体的なゴールは、不可視署名をオリジナルの映画762に、前記署名が並べ替わる、768によって記憶される前記映画の商業的価値を落とさず、前記署名がMPEG圧縮および伸張プロセスを経て最適に残存するように用いることである。上記で示したように、特にMPEGプロセスの使用が、圧縮の一般的なプロセスの一例である。また、ここで与えた例が、工業的変形に関して一定の能力を有することに注意すべきである。特に、動画圧縮の技術において実行されているこれらは、我々が2つのビデオストリームAおよびBで開始し、AおよびBを別々に圧縮し、これらの結果を結合する場合、結果として生じるビデオストリームCは、ビデオストリームAおよびBを単純に結合し、この結果を圧縮した場合とは一般に同じにはならないことが分かる。したがって、一般に、例えば、

$$\text{MPEG}(A) + \text{MPEG}(B) \neq \text{MPEG}(A+B)$$

となる。これは、本開示におけるこの点においていくぶん抽象的な概念を導入し、図15を論考するためにより明らかになるであろう。しかしながら一般的なアイデアは、圧縮手順の“不可視”署名の通過を最適化するのに使用できる種々の代数が存在することである。明らかに、図15に示すのと同じ原理は画像に依然として効果があり、JPEGまたは他のものが依然として画像圧縮の標準である。

【0218】

ここで図15の詳細に戻り、映画またはビデオのすべてのZフレームを通じて単純にステップすることから始める。一秒あたり30フレームで上置される2時間映画に関して、Zは、 $(30 \times 2 \times 60 \times 60)$ すなわち216000となる。700、702および7

0 4 の内部ループは、単に図 1 3 のステップの模倣である。ロゴフレームを、フレームのステップ任意に変更することができる。ボックス 7 0 4 から放射する 2 つの矢印は、ループ 7 5 0 の継続と、出力フレームのレンダリングマスタ雪状映画 7 5 2 への配置とを表す。

【0219】

この点において短いが可能的に適切な命題をすると、マルコフ処理の概念の使用は、図 1 5 の工業的実現化の最適化に関する議論をいくらか明確にする。簡単に、マルコフ処理は、イベントのシーケンスが短く、一般的に、このシーケンスにおける 1 ステップと次のステップとの間に記憶が存在しない処理である。図 1 5 の状況および画像のシーケンスにおいて、画像のマルコフのシーケンスは、所定のフレームと次のフレームとの間に明らかまたは多少の相関関係がないシーケンスである。これまでに制作されたすべての映画の組を取り、同時に 1 つのフレームをステップし、出力映画に挿入すべきランダムな映画からランダムなフレームを選択し、一分すなわち 1 8 0 0 のこれらのフレームを通じてステップすると仮定する。結果として生じる“映画”を、マルコフ映画の良い例とする。この論文の 1 つの点は、ロゴフレームをどのようにレンダリングするかに応じて、暗号化／スタンプ化ステップ 7 0 2 をどのように行うかに応じて、マスタ雪状映画 7 5 2 が、ある一般的な量でできる程度のマルコフの特徴を示すであろうことである。この点の要旨は、圧縮手順それ自身が、このマルコフの特徴の程度によって影響され、したがって図 1 5 の過程の設計において考慮する必要があることである。同様に、かつ単に一般的に、完全にマルコフ的な映画を高解度マスタ雪状映画 7 5 2 において形成したとしても、MP E G ボックス 7 5 4 として表されるその映画の圧縮および伸張処理は、7 5 2 のマルコフ的特性の根拠を減衰させ、少なくとも最低限に非マルコフ的な圧縮マスタ雪状映画 7 5 6 を形成する。この点を、本開示が 1 つの N ビット識別ワードを見つけるためにビデオストリームの多数のフレームを使用するアイデアを論じるときに使用し、すなわち、同じ N ビット識別ワードを映画のいくつかのフレームに埋め込むことができ、これらの多数のフレームから得られた情報を使用し、その 1 つの N ビット識別ワードを見つけることは、全く合理的である。したがって、7 5 6 の非マルコフ的特性は、前記不可視署名の読み出しおよび認識にいくつかの手段を加える。

【0220】

最終的に使用されるマスタ雪状映画 7 5 6 を前記論する目的により、ここで、レンダリングされた高解度マスタ雪状映画 7 5 2 を MP E G 圧縮および伸張手順 7 5 4 を経て送る。MP E G 圧縮は一般的に分配的でないと認められる上述した注意により、ステップ 7 5 4 のアイデアは、最初にレンダリングした雪状映画 7 5 2 を 2 つの成分、7 5 6 である圧縮処理 7 5 4 を免れる成分と、免れない成分とに大雑把に分離し、差映画 7 5 8 を使用して大雑把に推定し、“あっぽいマスタ雪状映画” 7 6 0 を発生することである。故意に散漫な言葉“あっぽい”を使用した理由は、恐らく共通の圧縮処理を免れないにも関わらず、圧縮を決して受けない用途または状況に対して“あっぽい”特別の署名信号エネルギーを発生できることを知ることにより、この署名信号を同様に配布可能映画後に付加することができるためである。(したがって、図 1 5 において少なくとも 1 示す。) 図 1 5 に戻り、我々は、圧縮処理を不変のまま残存する高い可能性を有することを加えている署名における荒い切断を行い、この“圧縮マスタ雪状映画” 7 5 6 を使用し、縮小した 7 6 5 であるこの手順を繰り返す、オリジナル映画と比較 (7 6 8) し、セットアップされているどのような商業的実行可能規準 (すなわち、許容しうる知覚されるノイズレベル) にも適合することを保証する。並べて観るステップ 7 6 8 から縮小ステップ 7 6 4 に戻る矢印は、図 2 の“規範的映画...”と、図 6 のゲイン制御 2 2 6 とに直接対応する。画像および音響処理における当事者は、図 1 5 の全体を、前記可視署名信号の、これらが完全に感知しうる圧縮さえもより耐えられるような前記調節を試みることによって要約できることを認識できる。上述した項目を同様に反復するため、このアイデアを、画像、音響シーケンスまたはオーディオトラックに受けさせてもよいからこのような前記識別可能処理に等しく用いる。これは、明らかに、静止画への J P E G 処理を含む。

【0221】

リアルタイムエンコーディング回路側の追加要素

一般に、ボックス750から展開マスタ雪駄映画の形成756を経て続く図15に示す方法ステップを、ある変更によって、ハードウェアにおいて実現することができることに注意されたい。特に、図6におけるアナログノイズ源206全体を、このようなハードウェア回路によって置き換えることができる。同様に、図13において示すステップおよび関係する手順を、ハードウェアにおいて実現することができ、アナログノイズ源206を置き換えることができる。

【0222】

2フレーム以上を基礎とする認識：非マルコフ的署名

画像のマルコフおよび非マルコフシーケンスにおける余剰において示したように、埋め込み不可署名品名を非マルコフ的性質である。すなわち、あるフレームのマスタ雪駄映像と次のフレームのそれとの間にある相関関係が存在し、さらに、1つのNビット識別ワードをフレームの範囲に渡って使用し、フレームのシーケンスに関連するNビット識別ワードのシーケンスが非マルコフ的特徴である状況において、1つのNビット識別ワードを認識するため、映画またはビデオのいくつかのフレームからのデータを使用できる点を、再び指摘する。このすべては、不可署名品を認識する原理は、動画像シーケンスの多数のフレームに変換する場合において、利用できる情報だけを使用すべきであるということを含む。この方法である。

【0223】

ヘッダ変形例

デジタル画像またはオーディオファイルにおける“ヘッダ”の概念は、当該技術分野において十分に確立された理論である。図16の上段は、ヘッダの概念における単純化した外観を有し、ここで、データファイルは、一般に、全体としてのファイルについての情報の包括的な組から始まり、しばしば、著作権者がいるなら、データの著者または著作権保持者である人についての情報を含み、このヘッダ800に、代表的に、オーディオストリーム、デジタル画像、ビデオストリームまたはこれらの項目の圧縮したもののようなデータそれ自体802が続く。これは、工業においてよく知られており、共通である。

【0224】

この技術の原理を情報保全のサービスに用いることができる1つの方法を、図16の下段に一般的に示す。一般的に、Nビット識別ワードを、画像（図示するような）またはオーディオデータストリーム全体の本質的に“壁紙”の所定の簡単なメッセージに使用することができる。これを、この節のタイトルにおける“ヘッダ変形例”と呼ぶ。ここで考へは、あまり洗練されていない著作権侵害志望者および悪用者がヘッダ情報の情報内容を変更することができ、したがってこのテクノロジのより安全な技術にヘッダ情報の真実性における検査として使用できることである。ヘッダにおける“ジョーの画像”のようなコードメッセージを付与した場合、ユーザが得る画像は、ヘッダの変更が行われないことと、あるより高い程度の信頼性を有することができる。

【0225】

同様に、前記ヘッダは、実際にNビット識別ワードを輸送することができるため、所定のデータセットをこのテクノロジの方法によって符号化したことを強調することができる。識別コードを前記ヘッダに正確に組み込むことができる。当然、このデータファイルフォーマットは、このテクノロジの原理が現在用いられていないことから、まだ形成されていない。

【0226】

“ボディア”：ヘッダの大きい変換に対する能力

本願人のテクノロジの以下の機能のすべての可能な用途が完全に開示されていないとしても、いくつか重要なかもしれない設計変更として与える。この節のタイトルは、この可能性を説明するために使用する勇腕な言い回し。“ボディア（BODIER）”を含む。

【0227】

前節では、Nビット識別ワードが、デジタルファイルのヘッダに含まれた情報をどのようにして識別するかについての概略を述べたが、これらの方法が、ヘッダの概念を完全に置き換えることができ、ヘッダに情報的に格納された情報を、デジタル信号および経験的データそれ自体に配置することができる予想も存在する。

【0228】

これを、単に例として、別の完全に経験的なデータストリームにおける96ビット(12バイト)リダストリングにおける標準化と同じ位簡単にすることができる。このリダストリングは、リダストリングを含まない全体のデータファイルの、要素のデータユニットにおける数字長と、1つのデータ要素の源生のビット数(例えば、クレイレベルの数またはオーディオ信号の離散的信号レベルの数)とを、明瞭かつ単純に含む。これらから、本明細書に記載の万能コードを使用し、経験的データ内に直接含まれたNビット識別ワードを読み出す。前記経験的データの長さは、完全なNビットを含むのに十分な長さとする必要がある。Nビットワードは、そうでなければ信頼的なヘッダに含まれるものを能率的に伝送する。

【0229】

図17は、このようなデータフォーマットを示し、これを“万能経験的データフォーマット”と呼ぶ。リダストリング820は、64ビットストリング長822と、32ビットデータワードサイズ824とから成る。次にすぐデータストリーム826が続き、ヘッダに情報的に含まれるが、ここではデータストリームには直接含まれない情報を、付加した点線828として表す。この付加した情報に使用した他の言葉は、図17にも示す“影チャネル”である。

【0230】

リダストリングに含めることが必要な他の要素は、データファイルの全体が変更されていないことを識別できる種の場合チェックサムビットである。

【0231】

配布された万能コードシステムにおける他：動的コード

万能コードのテーマにおける1つの興味深い変形は、万能コードそれ自体の動作を変更する命令を実行に含むNビット識別ワードの可能性である。多くの例のうちの1つは、データ送信を開始し、そこで、オーディオデータの所定のブロックが完全に伝送され、Nビット識別ワードを読み出し、5000の組から万能コード#145が使用するデータの第1ブロックと、このように見つかったNビット識別ワードの部分が、データの次のブロックを万能コードセット#145よりも#411を使用して分析すべきである命令であることを知る。一般的に、このテクノロジを、実際の復号化命令自体をオンフライで変更する方法として使用

することができる。さらに一般的に、“動的コード”を使用するこの可能性を、データ識別手順の洗練レベルを大きく上昇させ、ハッカーおよび著作権侵害者によってあまり洗練されていない妨害を受ける傾向があるシステムの経済的生存能力を増加させるべきである。本発明者は、復号化/暗号解読命令の動的変化的概念自体が新規であると信じていないが、経験的データの“影チャネル”におけるこれらの命令の実行は、本発明者の理解する限り、新規であると思われる。(影チャネルは、このテクノロジのよりシステムノックアウト的な適切な要素をカプセル化する他の専門的言い回しとして規定されている)。

【0232】

動的コードのテーマにおける変形は、その時どのコードを使用するかについての先天的に割り当てられた知識を有するシステムにおける万能コードの使用である。この可能性をまとめる1つの方法は、“ディリバスワード”のアイデアである。この例におけるバスワードは、どの万能コードの組が現在動作するかを加減を表し、これは、用途特定環境のある順に応じて変化する。恐らく、多くの用途が、万能コードをまだ一度も使用していないものに対して連続的に更新し、これは、ディリバスワードの情報的な機会よくある場合である。現在伝送されているNビット情報ワードの部分を、例えば、次の日のバス

ワードの経過とすることができる。例え、時間がパスワードの変更の最も普通のトリガイイベントであるとしても、同様にイベントを基礎とするトリガがあってもよい。

【0233】

対称パターンおよびノイズパターン：強固な万能符号化システムのために。

識別パターンの画像への配置は、確かに新しくない。画像のコーナースタンプされたロゴ、真の署名や著作権の丸記号のような複雑なパターン、および、透かしが、所有権を表すため、または、創造的題材の不正な使用を防ごうとするためにパターンを画像に配置することの例である。

【0234】

新規であると思われるものは、独立した“キャリア”パターンを配置するアプローチであり、これらのパターンは、それら自体を、ある情報と共に、前記情報の伝送および識別の目的のために画像およびオーディオに直接変調することができるともである。本発明者に現在既知のステガノグラフィ的解決法は、すべてこの情報を経験的データに“直接”配置する（できる限り最初に暗号化し、次に直接）が、本開示の方向は、これらの（非素にしばしば）同一空間キャリア信号の形成と、これらのキャリア信号の適切な情報との変調と、経験的データへの直接の適用とを規定している。

【0235】

これらの概念の拡張において、さらに万能コードシステムの用途の舞台に一步進み、ここでは、送信サイトは使用される特定の万能コード化計画によって経験的データを送信し、受信サイトは前記万能コード化計画を使用して前記経験的データを分析し、オーディオとは相違して画像または動画の伝送用に設計されたこのようなシステムの工業的理由において近い様子をとりとることが有利である。より明確に言うと、図9とこれに伴うオーディオ用途における万能コードについての論考に含まれるような特定の実現化の分析と同じタイプの分析を、画像（または2次元信号）にも同様にを行うべきである。この節は、万能コードの特定の実現化のこのような分析および戦略であり、このような方法が明らかにすべき種々のハードルを予測することを試みる。

【0236】

画像および動画用万能コード化システムの一実現化の統合するテーマは、“対称”である。これを進めるアイデアは、より簡単に、あまり洗練されていない著作権侵害者が、なにか与えられた万能コード化システムを迂回する意味として、画像データの使用に対する予防とすることはできない。先導する原理は、万能コード化システムを、従属する画像がどの回転方向であっても容易に読み取れるべきであるということである。これらの問題は、光学文字認識および物体認識の分野において共通であり、これらの分野を、このテクノロジーの工業的実現化の促進における他の方法および手段に関して参照すべきである。通常、直接的な例は順序である。

【0237】

デジタルビデオおよびインターネットカンパニーXYZは、入力ビデオを二重検査し、ビデオそれ自体の種々のフレームである複数のデータが、このテクノロジーを使用するXYZのそれ自体の比較的高い安全性の内部署名コードを含む、非対称万能コード化を種々の製品の配達システムを開発している。これは、ヘッダ情報が照合されると共にフレーム内万能コードが見つからなければどのような題材も通さない彼等のインターネット部門を含む、多くの配達状況において良好に働く。しかしながら、これらの商業的ネットワークの他の部分は、インターネットチャネルにおいて世界のルーチン監視を行い、彼等の所有の創造的財産の許可されない伝送を見つける。彼等は、使用される暗号化手順を制御し、したがって、ヘッダを含む創造的財産を暗号解読し、簡単な検査することは、彼等にとって問題ではない。XYZのネットワークにおいて題材を売買したい著作権侵害者グループは、XYZのヘッダ情報システムにおけるセキュリティ機能とをどのように変更するかを決定しており、さらに、1.0または2.0程度の画像を単純に照合させ、XYZネットワークに送信することによって、ネットワークは、コードを認識せず、したがって、彼等の題材の不正使用にフラグを立てず、著作権侵害者が回転した題材の受取人は、それを簡

単に回転しない。

【0238】

この最後の例を論理的な分類を経て要約すると、非対称万能コードは、“コードの発見を基礎とする許可された動作の可能性”に対して許可するものであるが、“コードの存在に関するランダムな監視（取締り）”の場合において多少容易にバイパスされる恐れがある。（非対称万能コードは、不正使用者の90%を極めて良好に捕らえることができる。すなわち、不正使用者の90%が単純な単純なバイパスをするに留まれないことを主張する）この後者の立場にアドレスするために、疑似回転対称万能コードの使用を必要とする。

回転問題を四角にする具年からの“疑心”装置は、この観測の変換において、完全に増加する回転対象オブジェクトを複雑な正方形格子において表すことはできない。さらに、基本的考察を、万能コードのスケール/大きさ変化に対して行う必要がある。監視プロセスを、監視される視覚的題材が“知覚”領域にある場合、すなわち、暗号化されておらず、スクランブル化されておらず、人間の見る人に対して与えられる（または与えられるであろう）形態にある場合、行う必要があることが理解される。著作権侵害意志者は、他の簡単なスクランブル化および非スクランブル化技術を使用することができ、道具を、これらの漏洩するスクランブル化信号を監視するために開発することができ、すなわち、著作権侵害意志者は、視覚的題材を知覚領域外に変換し、監視点によって通過し、前記題材を知覚領域に逆変換することを調査し、万能コードの監視と異なる道具が、このようなシナリオにおいて使用することが必要である。したがってここで考察した監視を、監視を知覚領域において行えるような用途に対して用い、このような場合、見る設備を実際に送る。

【0239】

“リンク”は、唯一の完全な回転対称2次元物体である。“ディスク”を、それらの半径軸に沿って面を有する同心で完全に接触しているリンクの単純な有限の組と見なすことができる。したがって、“リンク”を、画像に対するより堅牢な万能コード標準がそこから見つかる開始点とする必要がある。リンクは、スケール/倍率変更の問題にも良好に適応し、リンクの半径がそのトラックを保持し、聯通する1つのパラメータである。リンクの他の特性は、異なったスケール変化が画像における異なった空間軸に対して起こり、リンクが指門になる場合でも、どのような自動化監視システムも求めている滑らかな疑似対称特性の多くが一般的に維持されることである。同様に、どのような画像の通知しうる幾何学的歪みも、リンクを明らかに歪ませるが、これらは依然として全部の対称特性を保持することができる。うまくいけば、単純に画像を“観る”よりより平凡な方法で、これらの関係において、特に、このような長さが万能コード化システムをバイパスする場合、試みられた不正な著作権侵害を検出できるであろう。

【0240】

リンク対ノット

リンクを、その基礎に応じて完全無偏の堅牢万能コード化システムを構築できる唯一の理想的な対称パターンとして発見したことにより、我々は、この基本的なパターンを、情報を伝送でき、コンピュータまたは他の手段によって読み出すことができ、簡単な変換および改変を生じ抜くことができ、簡単なコスト増加項目としての破壊の経済性を保持するために、（万能コードにおける節で説明したように、恐らく増すことができない）高いレベルのセキュリティに合理的に上昇させることができる何か概念的な何かに変えなければならぬ。

【0241】

“リンクを基礎とする”万能コードの一例は、本発明者が、後に洗練され、レオナルド・ダ・ヴィンチの仕事（例えば、モナリザまたは彼のノット図案）において高められた、織られたケルトのノットパターンにしたがって、“ノットパターン”または単に“ノット”と呼ばれるのである。いくつかの頃は、ノットのこれらの結は、実際にステッチンググラフィックであり、すなわち、メッセージおよび署名、すなわち、より固有のもののすべてを伝達することをもたらし、図18および19は、これらのノットパターンの基本的な特性のいくつかを調査する。

【0242】

ノットパターンとの2つの簡単な例を、極放射ノット850および放射ノット852によって示す。これらの形式の名前は、底がったリングの中心の対称点と、構成するリングがこの点と交差するか、完全にその外側に、サブ放射ノットの場合、前記中心点構成する円の内部であるかどうかとを基礎とする。850および852の例は、明らかに、8個のリングまたは円の対称的配置を示す。“リング”を、上述したように、この言葉は、リングの放射軸に沿ったリングの幅を明白に認めるという点で、より広義の言葉とする。ノットパターン850および852における個々のリングは、我々のNビット識別ワードにおけるビットプレーンに関連する信号のためのキャリアや信号となるであろう。したがって、ノットパターン850および852の各々を、8ビット情報キャリアとする。特に、ノットパターン850および852を、黒い背景における明るいリングとすると、独立したソース画像への明るいリングの“加算”が“1”を表すことができる。独立したソース画像からの明るいリングの“減算”が“0”を表すことができる。この簡単な符号化計画の適用を、図19とそのノットパターンのモザイクにおけるように、何度も反復することができる。この符号化(変調化)ノットモザイクのスケールダウンバージョンを、オリジナル画像に直接かつ同一の時間に渡り追加する最終ステップと、この万能対称コード化方法を経て符号化された配布可能画像と結果とを伴う。どのリングが我々のNビット識別ワードにおける最下位ビットであり、どれが最上位ビットであるかを、復号化システムと通信することが残っている。1つのこのような方法は、(個々のリングの)半径値のスケールをLSBからMSBまでわずかに増加させることである。他の方法は、単に、MSBを他のものより10%大きい半径とし、残りのビットが一致しない順序としてカウンタクロック幅を予め割り当てることである。さらに他の方法は、ある簡単なハッシュマークをただ1つの円の内部に置くことである。すなわち、リングのビット順序をこれらのノットパターンにおいて符号化することができる種々の方法が存在する。

【0243】

最初にこれらのノットパターンの単なる存在に対して検査し、第2にNビット識別ワードの読み取る手順は、以下のようなものである。疑わしい画像を、最初に、極めて普通の2DFFTコンピュータ手順を経てフーリエ変換する。我々は、ノットパターンの正確なスケールを知らないとし、すなわち、我々は、画素の単位におけるノットパターンの要素のリングの直径を知らず、我々は、ノットパターンの正確な回転状態を知らず、我々は単に、警告する放射パターンに関するオリジナル画像のフーリエ変換の結果としての振幅(ソース画像の空間周波数プロファイルの頂点における同心低振幅正弦リング)を(基本的な自動化パターン認識方法によって)検査するとする。リングの間隔と共にこれらのリングの間隔性は、万能ノットパターンが存在すると思われるかまたは思われないかと、直素におけるこれらのスケールとを我々に知らせるのである。古典的な小さい信号検出方法としての目的に、この開示の他の検出方法を用いることができるように用いることができる。次に普通の空間フィルタ処理をフーリエ変換した疑わしい画像に用いることができ、ここで、使用すべき空間フィルタは、同心円の頂点におけるすべての空間周波数を通過させ、他のすべての空間周波数をブロックする。結果として得られるフィルタ処理画像を、空間周波数領域から空間領域にフーリエ変換し、ほとんど視覚的検査によって、明るいリングの反転または非反転を、MSBまたはLSBリングの識別と、N(この場合において8)ビット識別コードワードと共に見つけることができる。明らかに、パターン認識手順が、この復号化ステップを同様に行うことができる。

【0244】

前述の論考およびそれが説明する方法は、ある実質的な欠点と、ここで論議し改善する欠点とを有する。基本的な方法を、含まれる基本的な原理を伝えるために、素朴な様式において与える。

【0245】

ノットパターンを使用する上述した万能コード化システムのいくつかの実質的な困難を列挙しよう。一例として、(1)リングパターンは、全部の画像空間を“覆うこと”にお

いて、そして、簡便範囲の情報伝送容量のすべての使用において、いくぶん非能率的である。第2に、(2)リンクパターン自体が、これらを例えば8ビット白黒画像に対する単純な付加方法において用いる場合に、より可視である必要がある。次に、(3)図18の“8”リンクが850および852はむしろ少ない値であり、さらに、認識方法が対応する必要がある図に用いることができる22.5度の回転が存在する。次に、(4)リンクの完全な重なりが、加算され減算された輝度が安全に認知できるようにになってしまう。高く縮小された領域が発生する。次に、(5)復号化において使用した2DFFTルーチンは、言及されているパターン認識方法のいくつかと同様に、計算上扱いにくいことが有名である。最後に、(6)これにもかかわらず、ここまで説明した万能コード化の形態は、最高のセキュリティ通信システムの古典的なセンスにおける超高いセキュリティを有することを主張せず、それにもかかわらず、ハードウェアおよびソフトウェアにおいて実現するのに費用が増加せず。同時に、著作権侵害志望者がシステムの裏をかこうと試みる費用が増加し、これらの著作権侵害者に必要な洗練度レベルが上昇するという。ある程度のセキュリティ特徴を、著作権侵害志望者が、たぐらみ容易に証明され、うまくいけば(これらのノットパターンコードの創造的所有権を奪う手段の形成および配布のような)厳しい犯罪の責任および罰則を受けさせるシステムの裏をかか彼等の方法から進まなければならない点に対して、有利に付加する。

【0246】

これらの項目のすべてを取り上げることができ、前記テクノロジーの原理のどのような工業的実現化においても、改良しつづけるべきである。本開示は、以下の実施形態の参照と共にこれらの項目を取り上げる。

【0247】

項目番号3から始め、図18に示す8つのリンクのみが存在することを、単にリンクの数の増加によって補う。所定の用途が使用するのであるリンクの数は、明らかにその用途の関数である。トレードオフは、使用するリンクの数を制限することを主張する側において、少ないリンクが存在する場合、最終的にリンク当たり(可視度あたり)より多くの信号エネルギーが存在し、自動化認識方法によるその識別が容易になるように、リンクをあまり集めず、一般的に、これらはあまり集まっていないことから、全部のノットパターンを、より小さい全体の直素範囲、例えば、100直素直素領域よりも30直素直素領域を使用して含めることができるといったことを含むが、これらに限定されない。リンクの数を増加させる理由は、アスキー情報、シリアル番号、アクセスコード、使用可能コードおよび履歴情報、等のようなより多くの情報を伝送する要求を含む。より多くのコードを有することの他の便となる利点は、ノットパターンのそれ自体への回転が減少し、それによって、前記認識方法がより小さい範囲の回転角を捉えるようにすることである(例えば、64のリンクは、3度以下の最大回転変形を有する、すなわち、そのオリジナルパターンに対して最大に異なり、5.5度程度の回転は、ノットパターンをその初期アラインメントにならせ、MSB/LSBおよびビットプレーン順序を識別する必要性は、この例において同様によりよく理解できる)。大部分の実際的な用途は、Nビット識別コードワードにおけるビット数の選択に対する $N=16$ ないし $N=128$ に対応する16ないし128リンクを選択する。この選択の範囲は、850または852のような要素的ノットパターンに割り当てると、すべての半径と要素において幾分関連する。

【0248】

最後にあるリングパターンの集中と、他のことにおけるリングパターンの欠如(極めて類似しているが、項目1の非能率な例とは異なる)である実質的な困難の項目番号4を取り上げると、以下の改善を用いることができる。図18は、“ノット”(リンクのパターン)との対比としての線となる特徴の一例を示し、パターンが必ずしも変化する場所、仮想の第3次元を仮定し、それにより、ノットのある場所が、ある予め決められた方法において、他の場所よりも優先する(項目854参照)。他の見方から、ノットパターンにおける所定の交差点の輝度または暗さを、2つ以上の場所が重なる領域において1つの場所のみに“割り当て”る。このアイデアを、この割り当てについてのルールをある

回転対称方法においてどのように行うかに拡張する(864)。例えば、ルールを、時計方向に選べることにより、ループに入ってくるひもが、出ていくひもの後方になることにする。明らかに、これらのルールに用いることができる多数の変形例が存在し、その多くは、選択したノットパターンのジオメトリに決定的に依存する。余される他の問題は、恐らく、有眼の幅と、さらに、ひもの方向に対して垂直の軸に沿った幅の離度プロファイルとが、ノットパターンの下にある所定の義歯への離度割り当てのルールにおいてそれぞれ役割を演じることであろう。

[0249]

上述した名目上のノットパターンシステムに対する主要な改善は、実質的な困難、(1) 非能率的に覆うこと、(2) リングの望ましくない可視度、および(6) 高いレベルのセキュリティの必要性を直接取り上げる。この改善は、直前の節において論考した項目(4) 重要な問題も間接的に取り上げる。この主要な改善は、以下の通りである。符号化ノットパターンのモザイクをオリジナル義歯に付加し、配布可能画像を発生するステップの前に、符号化ノットパターンのモザイク866を、標準化され、(一般的に滑らかに)ランダムな位相のみの空間フィルタによって、(普通の2D FDF技術を使用して)空間的に回転対称である。この位相のみのフィルタが、空間周波数領域においてそれ自体完全に回転対称であり、すなわち、そのフィルタ処理作用が完全に回転対称であることに注意することは、極めて重要である。個々の離度リングにおけるこの位相のみのフィルタの作用は、同心リングの滑らかに変化するパターンに変換し、このパターンは、右を露とした後のいくつかの場合における水上のパターンとまったく異なってはならず、波パターンが、この位相のみのフィルタの場合において、右波パターンの一種な周期性よりも、いくぶんランダムである。図20は、これらの位相のみフィルタ処理化リングパターンの粗い(すなわち、非クレイスケールの)表現を与える。図20の上部の図は、これらの位相のみフィルタ処理化リングパターンの1つの代表的な離度輪郭/プロファイルの断面図874である。個々のリングの中心872を、これらのフィルタ処理化パターンの1つの2次元離度分布を完全に記述するために、前記離度プロファイルをその回りで回転させる点とする。フィルタ処理化リングの特性を伝えるさらに他の粗い試みを、フィルタ処理化リングの大雑把なクレイスケール義歯876として表す。この位相のみフィルタ処理化リング876を、ランダム波状パターンと呼ぶことができる。

[0250]

図20に示さないことは、図18のノットパターンまたは図19のノットパターンのモザイクにおける位相のみフィルタ処理の合成作用である。ノットパターン850または852における各々のリングは、876の形式の2Dの離度パターンを生じ、一緒に、ある程度複雑な離度パターンを形成する。リングの符号化を、明らに(1) または“粗い”とすることによって行うことによって、結果として得られる位相のみフィルタ処理化ノットパターンは、人間の眼にはもはや感知できないが、特に、位相のみフィルタ処理をオリジナルリングパターンを再生する逆フィルタ処理した後、コンピュータには容易に識別できる顕著な特徴を取りはじめる。

[0251]

ここで図19に戻ると、我々は、8ビット識別ワードをノットパターンにおいて符号化し、ノットパターンを位相のみフィルタ処理したことを想像できる。結果として得られる離度分布は、ある美しさを有するが、眼/脳には容易に分らない重要な波パターンの要素をタペストリである。(これに対する例外は、南太平洋島国間の知識から引き出すことができ、航海者は、原始的な航海手段として、分散され反射された間にある島々の渾身の島の波によって発生された、小さく、増加する複雑な海の波パターンを読み取る顕著な技術を手伝ったと言われている。) よりよい言い回しの要求に関して、結果として得られる(866から得られた) フィルタ処理化ノットパターンのモザイクを、符号化ノットタペストリまたは単にノットタペストリと呼ぶことができる。このノットタペストリの幾つかの基本的な特性は、その発生するモザイクの基本的な回転対称性が保持されることと、一般的に、眼/脳には分らず、したがって、逆問題工字の複雑レベルにおける段階を高め

ること、画素の格子の利用可能な情報内容の使用において、より能率的である（次の節においてより重要である）ことと、基本的なノット概念8×4および8×4を使用する場合、信号レベルが波状に集中し、したがって視聴者に不快に可視になる“ホットスポット”が発生しないことである。

【0252】

上述した基本的な良好化処理は、符号化処理において使用した位相のみフィルタを逆フィルタ処理する追加のステップを必要とする。この逆フィルタ処理は、画像処理産業においてよく知られている。ノットパターンにスケールが先天的に分かっているとなると、逆フィルタ処理は簡単である。他方で、ノットパターンにスケールが分かっていない場合、このスケールを見つける追加のステップが適切である。ノットパターンにスケールを見つける1つのこのような方法は、逆の位相のみフィルタを、復号化している画像の種々のスケールのバージョンに反復的に適用し、顕著なノットパターンを示し始めるスケールバージョンを捜すことである。単体方法のような普通の探索アルゴリズムを、パターンにスケールを正確に見つけるために使用することができる。物体認識の分野も、スケールが分からない物体検出の一般的な表題の下に参照すべきである。

【0253】

ノットタペストリが画像画素格子を覆う能率についての追加点の概要である。万能画像コード化のノットタペストリ方法の大部分の用途は、完全に符号化されたタペストリ（すなわち、埋め込まれたNビット識別ワードを有するタペストリ）の用途を、比較的低解像度レベルにおいて、ソース画像中に置く。実際の言葉において、符号化タペストリの解像度スケールが、例えば、代表的な256クレイスケール画像において5クレイスケール値から5クレイスケール値で変化し、ここで、値の傾斜は-2ないし2となる。これは、ノットタペストリが通知しうるビット切断エラーを受ける単に実用的な方法をもたらす。例として、完全な256クレイスケール画像を良好に使用し、これを解度において係数20によってビット切断ステップを含むスケールダウンをし、このビット切断バージョンを解度において同じ係数20によって再スケールし、その結果を逆の位相のみフィルタ処理して構成されたノットタペストリを画像する。結果として得られるノットパターンモザイクは、オリジナルノットパターンモザイクの調音に劣化したバージョンとなる。このすべてを持ち出す点は、以下の通りである。簡単に規定されるが、実際にはノットタペストリ方法の実現化における設計の種々の自由パラメータを選択する工業的タスクに挑戦し、最終的な目的は、ノットタペストリのある予め規定された可視度許容率内で、Nビット識別ワードについての情報の最大量を通過させることである。前記自由パラメータは、画素における要素的リングの半径と、Nすなわちリングの数と、画素におけるノットパターンを中心から要素的リングの中心までの距離と、あるノットパターンに他のノットパターンとの詰め込み規則および距離と、ひもの織り方に関するルールと、ノットモザイクに使用するべき位相のみフィルタの形態および形式とを含むが、これらに限定されない。このようなパラメータを、これらの選択において助けになるコンピュータ最適化ルーチンに供給することが望ましい。これは、含まれる多くの非線形自由パラメータにより、科学よりも芸術として始まる。

【0254】

位相のみフィルタ処理の使用における付随する注意は、リングパターンの検出において援助することができることである。前記符号化プロセスの逆のフィルタ処理は、ノットタペストリを付加する。下にあるソース画像を“曖昧”にする傾向があり、同時に、リングパターンを“フォーカスする”傾向がある。ソース画像の曖昧化がなく、現れるリングパターンは、代表的な画像の解明的特徴に“対抗”する。より困難な問題を有する。前記符号化手順は、他の節において説明した図解とも値化方法も使用すべきである。簡単に、これは、ソース信号が解度において費々の署名信号より大幅に大きいことが分かっている場合、復号化している画像は、署名信号の信号レベルをソース信号に対して上昇させるサービスにおいて、より高い分配領域きい値を有することができる方法である。

【0255】

上述した他の光学的な図解である。2D-FFTルーチンおよび代表的なパターン認識ルーチンの相対的な計算上のオーバヘッドに關する項目(5)に関して、ここに置くが満たされない最初の成功の案は、リンク確率の確性を、2D-FFTを使用するよりも迅速に認識し、復号化するより簡単な方法を見つけることである。これを除くと、個々のノットパターン(850または852)の画像範囲を、例えば直徑において50画素とした場合、画像のある部分における簡単な64倍の64画素の2D-FFTは、上述したNビット識別ワードを識別するのに十分であることが分かる。このアイデアは、Nビット識別ワードを識別するために、画像全体を使用することが必要であると相違して、必要な最小の画像領域を使用することである。

[0256]

他の注意は、画像処理の科学におけるこれらの弁護士がリンクの使用を伴うノットパストリにおける議論を始める代わりに、我々は、QUAを基礎として機能する2D確度分布パターン876の使用に真直ぐに飛ぶことができる。ベースライン技術としての“リンク”という用語の使用は、いずれにしても発明開示に関して適当であるため、厳格教訓的である。より重要なことは、ひょっとすると、逆フィルタ処理後の復号化処理における真の“リンク”の使用が、おそらく、代表的なパターン認識ルーチンに入力する最も簡単な形態であることである。

[0257]

ニューラルネットワークデコーダ

信号処理の当業者は、ニューラルネットワークアーキテクチャを用いるコンピュータが、本特許ノロジーによって提出された、パターン認識およびノイズにおける最小信号の検出問題に好適であることを認識するであろう。これらの題目における完全な開示は本明細書の範囲を越えており、興味を持った読み手は、例えば、チャカスキー、ワイ、 “統計学からニューラルネットワーク：理論およびパターン認識導出”，スプリングerverlag、1994；マスターズ、ティ、 “ニューラルネットワークによる信号および画像処理：Cソースブック” ウィレイ、1994；ティオン、アイ、 “ニューラルネットワークシステムを使用するパターン認識における進歩”，ワールド サイエントフィックパブリッシャーズ、1994；ニダリン、エイ、 “パターン認識用ニューラルネットワーク”，ウィレイ、1993；およびチェン、シー、 “パターン認識用ニューラルネットワークおよびそれらの用途”，ワールド サイエントフィックパブリッシャーズ、1991を参照されたい。

[0258]

2D万能コード：一次元の場合の単純走査ライン実装化

リンク、ノットおよびタペストリーにおける上記は、確かにその美しさを有するが、含まれるステップの幾つかは、実効的な実装化が、ある用途に対して費用が掛かりすぎてしまう程の複雑さを有するかもしれない。リンクおよび良設計された対称性の概念の粗末な類似は、図9およびオーディオ信号に関連して与えた基本的概念を単純に使用し、これらを画像のような二次元信号に用いるが、例えば、画像における各々の走査ラインが、例えば、100画素長万能ノイズ信号においてランダムを開始点を有するように行うことである。識別ソフトウェアおよびハードウェアは、回転状態およびスケール係数の完全な範囲を横切る後を質問し、これらの万能コードの“存在”を見つける義務がある。

[0259]

万画商用著作権(UCC)画像、オーディオおよびビデオファイルフォーマット

よく知られているように、過多数のデジタル画像、デジタルオーディオおよびデジタルビデオに関するファイルフォーマット標準(および標準でないもの)が存在することは既知である。これらの標準は、一般的に、特定の産業および用途内で形成されており、放散した創造的デジタル権利の使用および交換のため、種々のファイルフォーマットが、交互の標準のための間接性において益しく無い。そこで今日、我々は、種々の気に入っているフォーマットの無秩序的なファンおよびユーザーの事実上のストグラムを見る。フォーマット化および圧縮のためのJPEG、MPEG標準は、ある計画された産業間の共同

研究が活動しはじめる場合に見ることができ、わずかな例外に過ぎない。

【0361】

オーディオ/ビジュアルのための標準的万能標準ファイルフォーマットに対する切望は、非常に古い。このような題材の保護に対する切望は、なおさら古い。万能フォーマットの形成に伴う固有の困難に関して、そして、特許開示中のこのような計画の商業的物体よりに関して、本発明者は、これらの方法が、ひとことすると、一般に認められた世界的な“万能商用著作権”フォーマットを構成する基礎となるなにかと類似に役に立つことができると信じている。発露士は、このような動物が、宣言によって形成されず、広いニーズ、困難および幸運の能率的な集合を通じて形成されることを知っている。この開示の目的により密接に関連することは、このテクノロジーの用途が、産業標準ファイルフォーマット内の中心的な部分になる場合、利益を得ることである。特に万能コードの使用を、このような標準内に指定することができる。このテクノロジーの商業的習慣の最大限の表現は、不可視署名を行い、信用を著作権保持者に吹き込む知識から来ている。

【0361】

以下は、このテクノロジーの原理がこのような標準に対する触媒として働くことができる理由のリストである。(1) いるとしてもほとんどない技術的開発者が、経験的データおよびオーディオ/ビジュアル題材の不完全な保護の問題を認識し、明白にアドレステス。(2) すべての上述したファイルフォーマットは、データについての情報と、データ自体とを、2つの分離して物理的に異なった存在として取り扱っているが、このテクノロジーの方法は、これら2つを1つの物理的存在に結合することができる。(3) このテクノロジーの原理の大スケール用途は、まず第1に、圧縮テクノロジーにおける未来の改善による統合を含む、実用的な標準化作業を必要とし、その結果、標準の基盤が存在しなくなる。(4) マルチメディアの発露は、“内容標準”のますます高いレベルを論じる、テキスト、画像、サウンドおよびグラフィックスを含む“内容”と呼ばれるデータの属性クラスを形成した。(5) 著作権保護テクノロジーおよびセキュリティ特徴をファイルフォーマット標準に直接結合することは、長い間遅れている。

【0362】

万能標準の要素は、前記ヘック証明方法の幾何的な特徴を必ず含み、ここで、ヘック情報を、直接にデータ内の署名コードによって識別する。また、万能標準は、完全に秘密のコードおよび公開コードの混成使用をどのように混じり合わせるかの戦術を述べる。したがって、公開コードを赤裸裸された著作権侵害者によって“取り除かれた”場合、秘密コードは元のままである。万能標準は、不可視署名が、デジタル画像およびオーディオが発展するにつれてどのように発展するかを指定する。したがって、所定の画像を、いくつかのソース画像を基礎として形成した場合、前記標準は、古い署名をどのように何時取り除き、新たな署名によって置き換えるかと、前記ヘックがこれらの発展の記録を残すかどうかと、署名自体がある種の記録を保つかどうかとを指定する。

【0363】

産業的実用

本開示の大部分は、Nビット識別ワードの基本的キャリアである産業に焦点を置いている。1つの“マスタコード信号”の使用を論じる節は、各々のそしてすべての産業をNビット識別ワードにおける固有のビットプレーンに本質的に“割り当て”点まで行っている。

【0364】

多くの用途に関して、インチ当たり300ドットの解像度におけるインクを基礎とする印刷の用途である一例によれば、原始的なデジタル画像ファイルにおける画像が実際に（例えば、一枚の紙においてデジタル化されたインク）染みになる。しばしば、オリジナル画像の容量を転送する独立した情報は、隣接する画像が、オリジナル画像の幾何学的に規定された空間にこぼれることによって変換される。当業者は、これを、簡単な空間フィルタ処理および、ブラーリングの種々の形態として認識するであろう。

【0365】

このような状況において、単に1つの画素よりも、特定の画素の極めて局所的なグループ（Nビット識別ワードにおける固有のビットパターンにより有利に割り当てることが出来る。最終的な目的は、単に、署名信号エネルギーのより多くを、より低い周波数に予め集中し、大部分の実験的な実現化が、より高い周波数を迅速に取り除く、または軽減することを実現することである。

【0364】

素朴なアプローチは、1つの割り当てられた画素を変調するよりも、変調すべきすべての画素の2倍の2つのブロックに同じ基本的な署名クレイ値を割り当てることである。より上等なアプローチを図21において示し、ここで画素グループのアレイを示す。これは、配置の大きなクラスの特定の例である。このアイデアは、画素の特定の小さな領域をNビット識別ワードにおける所定の固有ビットパターンに関連させ、このグループ化が、ビットパターン間の画素を実際的に共有する（画素画素の2倍の2つのブロックの場合のように、画素を共有する必要がないとしても）ことである。

【0367】

図21に示したものは、一例の正規化重み付けを有する、画素の3倍の3アレイである（正規化合計1になる重み）。このテクノロジーの方法は、1つの画素におけるよりも、単位として、この要素の「突起」において動作する。この例において、署名信号の拡張により、格納することが必要なマスタコード値の数において4倍の減少があることが分かる。不可視署名における配置に対するこの「突起アプローチ」の用途は、先天的に既知の多量のプラーニングを経験し、この激しいプラーニング後においても正確な識別を求められるいかなる用途をも含む。

【0368】

このテクノロジーのステガノグラフィの使用におけるその他の

本開示の初めの節において言及したように、技術および科学としてのステガノグラフィは、このテクノロジーに対する一般的な先行技術である。ここで、立場を述に、ここまで冒険してきた読み手にはすでに疑いなく明白であるように、このテクノロジーの方法を、ステガノグラフィを行う新規の方法として使用することができる。（なるほど、ここまでの考察のすべては、ステガノグラフィの種々の形態および実現化を調査することに関係している）。

【0369】

本節において、我々は、ステガノグラフィを、メッセージを点Aから点Bに伝える必要性として考え、このメッセージを、一般的に独立の経験的データ内に本質的に隠されているとする。遠隔通信の産業における誰かが証明できるため、メッセージを伝える目的の範囲をかなり広げる。恐らく、これらのメッセージをなんらかの数の例外的に簡単なチャネルを経て送信するよりも、純粋な趣味の他に、ある例外的な必要性があるであろう。ステガノグラフィにおける過去の文獻および製品宣伝は、特にこのような例外的な必要性を、メッセージがまさに送られている事実を隠すことに対する要求としているかもしれない。他の可能な必要性は、例外的な通信チャネルが直接利用できないが、費用的に禁止されるとして、すなわち、メッセージの送り手が彼等の符号化経験的データをどうにかして“送信”ことができることである。この開示は、参照により、ステガノグラフィを用いることができる無数の使用におけるすべての以前の考察を含み、本発明者がまだ説明していない以下の使用を追加する。

【0370】

第1のこのような使用は、きわめて簡単である。その中でメッセージを送る経験的データについてのメッセージを送ることが必要である。ある以前のステガノグラフィ実行者がすでにこの冗誼を利用していないことが、決して不可能であるとしても、ささいな冗誼は、媒体が既にメッセージである。経験的データについての情報をその経験的データ内に直接配置することにおけるある考察は、ヘッタを交換することにおける節と、“ポディヤ”の概念とにおいて既にカバーされている。

【0371】

経験的データについてのメッセージをそのデータ内に直接配置することの利点は、データオブジェクトの、以前の2つのクラスよりも、ただ1つのクラスが存在することである。そのような2クラスシステムにおいても、2つのクラスが無関係になるか、一方のクラスが他方のクラスがそれについて知ることをなしに再感染される危険性が存在する。具体的な例は、本発明者が“装置独立命令”と呼ぶものである。

【0272】

無数の機械データフォーマットおよびデータファイルフォーマットが存在する。このフォーマットの過半数は、万能データ交換に向かう進歩を妨害するそのパワーと、ある機械は、他の機械ができることと同じことを行っていることにおいて悪名が高い。創始者がデータの第2クラス（すなわちヘッダ）に用いたかもしれない命令は、これらの命令を認識するようにした機械に少しも適合しないかもしれない。フォーマット交換を行った場合、決定的な命令が、この進路に沿って取り除かれるか、混乱するかもしれない。ここで開示した改善を、命令およびメッセージを認識するために読み出し機械によって必要とされるすべてが、経験的データにおける標準化“認識アルゴリズム”を行うものとなるように、特定の命令を経験的データに直接“封印する”方法として使用することができる（もちろん、機械は、経験的データ特性を少なくとも“読む”ことができる）。すべての機械は、このアルゴリズムを、これらが選択したなんらかの古い方法で、なんらかのコンピュータ、またはこれらが必要とする内部データフォーマットを使用して実現することができる。

【0273】

この装置独立命令方法の実現化は、一般的に、メッセージに封印されたものの著作権侵害または不正な除去の問題を考慮していない。恐らく、埋め込まれたメッセージおよび命令は、題材の基本値および機能における中心的な大切な部品となるであろう。

【0274】

本テクノロジーの一種のステガノグラフィ的な使用の他の例は、ユーザー共同体の利益のための万能使用コードの埋め込みである。伝達されている“メッセージ”を、単に、経験的情報の正当な使用および支払いを望むユーザーに対して所有権を認める登録シリアル番号とすることができる。このシリアル番号は、所有者の名称や、直付け情報や、請求情報、等を含む創造的特定の莫大な登録に見出し付けすることができる。前記“メッセージ”を、所定の題材に関する自由および公的な使用の許可とすることもできる。同様の所有者識別および使用インデックス化を、ヘッダのような2クラスデータ構造方法において達成することができるが、このテクノロジーの1クラスシステムの使用は、前記1クラスシステムが、ファイルフォーマット交換、ヘッダ互換性、内部データフォーマット問題、ヘッダ/ボディアーカイビング問題、および媒体変化を気にしないという、前記2クラスシステムを越えるいくらかの利点を提供することができる。

【0275】

完全に正確なステガノグラフィ

本発明者に現在既知の先行技術のステガノグラフィ技術は、一般的に、メッセージを伝達する完全に決定的、すなわち“正確”な変換を含む。すなわち、これは、完全に正確に伝達すべき所定のメッセージに関して、情報の受け手は、送り手によって送られた正確なデジタルデータファイルを受け取る必要があり、ビットエラーまたはデータの“損失”を許容することが、基本的な仮定である。定義により、経験的データにおける“損失的”圧縮または増強は、このようなステガノグラフィ的方法を無効にする。（上述したコマツの工事のような先行技術は、ここでは例外とする）。

【0276】

このテクノロジーの原理を、ステガノグラフィ固有の正確な形態として利用することができる。先行技術またはこのテクノロジーのようなステガノグラフィの正確な形態は、“デジタル署名”および/またはDSS（デジタル署名標準）の比較的新しい技術と、所定の経験的データの受け手は、情報の元のビットも受け取ったファイルにおいて変化していないことを最初に確かめることができ、したがって、含まれる正確なステガノグラフィ的メッセージが変化していないことを確かめることができるように結合されることが暗

示される。

【0271】

正確なステガノグラフィ的システムにおいてこのテクノロジの原理を使用する最も簡単な方法は、マスタ雪駄コードがゼロを含むことを許可されない、上述した“設計された”マスタノイズ計画を使用することである。情報の送り手および受け手の双方が、前記マスタ雪駄コード信号およびオリジナル信号化オリジナル信号の双方にアクセスする必要がある。符号化信号の受け手は、単に、オリジナル信号を減算して差信号をとり、前記差信号とマスタ雪駄コード信号との間の簡単な確率検査の技術が、データ標本毎に、伝達されたメッセージを同時に1ビット発生する。恐らく、グレイ値範囲の“ルール”に近い値を有するデータ標本は、(8ビット深さの経験的データにおいて値0、1、2、4および255のように)取り除かれる。

【0272】

統計的ステガノグラフィ

ステガノグラフィ的に埋め込まれたデータファイルの受け手に対する、オリジナル信号へのアクセスを有する必要性は、本発明者が“統計的ステガノグラフィ”と呼ぶものに類することによって取り除くことができる。このアプローチにおいて、このテクノロジの方法を、埋め込まれたメッセージを探索する経験的データセットの読み出しを支配する単純な先天的ルールと用いる。この方法は、DSSによるようなデータファイルの完全性を識別する先行技術の方法と組み合わせても良好に使用できる(例えば、ワルトン、“不安定な新時代のための画像認証”、ドクター トプス ジャーナル、1995年4月、標本ずつ、ビットずつ、デジタル画像の完全性を識別する方法に関する18ページを参照されたい)。

【0273】

統計的ステガノグラフィは、送り手および受け手の双方が、同じマスタ雪駄コード信号へのアクセスを有する。この信号を、完全にランダムで確率的に双方のパーティに送ることができ、または、より大い疑似ランダムマスタ雪駄コード信号を発生する。共有され安全に送信されたより低いオクターブのキーによって発生することもできる。メッセージの16ビットの固まりは、経験的データの隣接する1024標本ブロック内で伝達され、受け手は、本開示において概要を述べたようなドット積復号化方法を使用することが、先天的に規定されている。情報の送り手は、ドット積アプローチが正確な16ビット値を実際に発生することを、予め検査する(すなわち、送り手は、キャリアや直値とメッセージ信号との間のクロストークが、ドット積動作がどの16ビットの望ましくない収束も発生するようなものでないことを予め検査する)。ある一定の敷1024の標本ブロックを送信し、したがって16ビットのメッセージを同じ数の回数送信する。DSSテクニックを使用し、送信されたデータがデジタル形態における存在に対してのみ既知である場合、メッセージの完全性を識別することができ、それは相違して、内部チェックサムおよびエラー訂正コードを、データがその送信において変化および交換されるかもしれない状況において送信することもできる。この後者の場合において、所定のメッセージ内容サイズに対して標本のブロックをより長くする(単に例として、16ビットメッセージ固まりに対して10K標本のようにする)ことが最適である。

【0280】

エラー訂正ステガノグラフィの話題における時間を省くこと、ここに開示された多くの復号化テクニックは、符号化データによって増加した要素(または冗余)を、符号化データによって減少したこれらから識別する原理において動作することが認識されるであろう。これらのポジティブおよびネガティブな場合の識別は、デルタ値(例えば、符号化要素と対応するオリジナル要素との差)がゼロに近づくにつれて増加して困難になる。

【0281】

類似した場合は、曖昧な中間クランドが2つの所望の信号基盤(例えば、+/-1)に分離する。特定のモデム送信技術において発生する。この中間クランドの誤った判断から得られるエラーは、時々“ソフトエラー”と呼ばれる。モデム技術およびこのような問題

が発生する技術からの原理を、同様に、現在の状況におけるこのようなエラーの軽減に用いることができる。

【0283】

1つのアプローチは、各々のデルタ周知の“信頼性”に重み付けすることである。両素（突起）が明らかにある状態または他の状態（例えば、 $+1/-1$ ）をもたず場合、その“信頼性”をハイであると言い、比例してより大きい重み付けを与える。反対に、両素（突起）がその判断において比較的曖昧である場合、その信頼性は相応してより低く、比例的により小さい重み付けを与える。その信頼性値に従って各々の両素（突起）からのデータを重み付けすることによって、ソフトエラーの影響を大幅に減少させることができる。

【0283】

このような信頼性重み付けを、他のエラー検出/訂正計画に対する有用な補助として使用することもできる。例えば、既知のエラー訂正多項式において、上述した重み付けパラメータを使用し、エラーの場所の多項式を基礎とする誤差をさらに減くすることができる。

【0284】

ベクトルグラフィックスおよび極めて低いオクタのインデックス化グラフィックスにおける“ノイズ”

この開示の方法は、一般的に、“経験的データ”の存在を仮定し、これは、ほとんど定義によってそれらに含まれるノイズを有する信号を言い表す他の方法である。一般的に、先天的にノイズを有するとは考えられない2次元グラフィックスの2つのクラス、すなわち、ベクトルグラフィックスおよび特定のインデックス化ビットマップ化グラフィックスが存在する。ベクトルグラフィックスおよびベクトルグラフィックファイルは、一般的に、コンピュータまたはプリンタが、直線、曲線および形状をどのように描写するかについての正確な命令を含むファイルである。このようなファイルにおける1ビット値の変化は、極めて大雑把な例として、円を四角に変えるかもしれない。すなわち、一般的に、これらのファイル内に利用する“先天的ノイズ”が存在しない。インデックス化ビットマップ化グラフィックスは、PCコンピュータにおける初期のCGAディスプレイにおける16のように、一般的に少ない数の色またはグレイ値から成る画素に属する。このような“極めて低いオクタ”のビットマップ化画素は、通常、自然界のカメラによって撮ったデジタル画素の試みられた表示において使用するよりも、グラフィックスおよびマンガを表示する。これらの形式の極めて低いオクタのビットマップ化グラフィックスも、一般的に、古典的なセクスの言葉における“ノイズ”含むとは考えられない。例外は、“ノイズ”の概念が依然として有効であり、このテクノロジーの原理が依然として有効である。インデックス化グラフィックファイルが、GIF（コンピュータのグラフィック交換フォーマット）によるような自然画像を表現しようとする場合である。これらの後者のフォーマットは、しばしば、（点描印刷およびカラー新聞印刷と同様の）ディザリングを使用し、実物に近い画像を生成する。

【0285】

この面は、慣例的に“ノイズ”を含まない2次元グラフィックスのこのクラスを考察する。この面は、このテクノロジーの原理を、どのように依然としてある方面においてこのような創造的題材に適用できるようにするかについての簡単な様子を取り上げる。

【0286】

このテクノロジーの原理をこれらの“無ノイズ”グラフィックスに用いる最も簡単な方法は、これらを、このテクノロジーの原理の用途に従う形態に変換することである。多くの言葉が、この産業において、ベクトルグラフィックをグレイスケールの画素を基礎とするラスター画像に変換するよう、ベクトルグラフィックの“リッピング”を含む、この変換に使用されている。アドビによるフォントショップのようなプログラムは、ベクトルグラフィックをRGBまたはグレイスケールデジタル画像に変換する。このような内部リソースを有する。一度これらのファイルをこのような形態に変換すると、このテクノロジーの原理を簡単な方法で適用することができる。同様に、極めて低いインデックス化ビットマップ

アを、RGBデジタル画像または同等物に変換することができる。RGB領域において、前記署名を適用したにおいて3つのカラーチャネルに用いることができ、または、RGB画像を、アビビのフォトショップソフトウェアにおける“ラフ”のよう各チャネル/クロマフォーマットに簡単に変換することができる。前記署名を“明るさチャネル”に用いることができる。ビデオテープ、CD-R、ROM、MP3、MP4、デジタル画像、および印刷のような媒体の大部分が、このテクノロジーの原理の用途に供する形態であるため、ベクトルグラフィック形態および極めて低いオーダのグラフィック形態からのこの変換は、何らかのイベントにおいてしばしば行われる。

[0287]

このテクノロジーの原理をベクトルグラフィックスおよび極めて低いオーダのビットマップ化グラフィックスに用いる他の方法は、根に対してノイズとして現れるこれらの先天的なグラフィックフォーマットに対する特定の特性が存在することを認識することである。最初の例は、所定のラインまたは形状が描かれているまたは描かれていない場所、または正確に、ビットマップが経から変化する場所の境界および輪郭である。大部分の場合において、このようなグラフィックスの人間の視覚者は、グラフィックオブジェクトの正確な輪郭の厳密で組織的な変化による“変調署名信号”のいかなる試みにも鋭く気付くであろう。それにもかかわらず、このような署名の符号化は、実際に可能である。このアプローチと、この開示の大部分において開示されているものととは、ここでは、署名を、純粹に別個に形成したり信号に追加するよりも、最終的に所定のグラフィックにおいてすでに存在するものから得なければならぬことである。この開示は、それにもかかわらずここで可能性を指摘する。基本的なアイデアは、輪郭、右方接触または左方接触、上方接触または下方接触を、Nビット識別ワードを伝達することのように変調することである。ノイズが、所定の輪郭に垂直な方向または他の方向のランダムな空間シフトの記録であるとしても、変化する輪郭の場所は、類似のマスクノイズ画像に含まれる。Nビット識別ワードのビット値を、用いられた変化とマスクノイズ画像に記録された変化との同値性検査を使用して、符号化し、読み出す。

[0288]

本テクノロジーの原理を基礎とするプラスチッククレジットおよびデビットカードシステム

プラスチッククレジットカードと、より最近ではデビットカードおよびATMキャッシュカードとの使用における発限は、ほとんど前書きを必要としない。ここでこれらの金融手段の詐欺および不正使用の長い歴史について多く議論することも必要ない。クレジットカードはホログラムの発展と、その後の偽造物の発展とは、プラスチックカードセキュリティ手段および不正な付抗策のギャンブルの歴史的な例として述べている。この節は、それ自身が、このテクノロジーの原理を、選択的に高度に耐詐欺的でありながら費用効果的なプラスチックカードを基礎とする金融ネットワークにおいてどの様に実現できるかに関する。

[0289]

現実的なプラスチック経済に関する所望の特徴の基本的なリストは、以下の通りである。1) 所定のプラスチック金融カードは、偽造することが完全に不可能である。2) 試みられた偽造カード（良く似ている）は、処理環境においてまったく機能することができない。3) 著作権侵害者等によって妨害された電子処理は、どのようにも有効とならず、または再使用可能にならない。4) 実際の有効なカードの物理的盗難の事象において、盗難者がそのカードを使用するのを依然として強力に阻害する。5) 金融カードシステムの全体的な経済的費用が、現在の典型的クレジットカードネットワークと等しいかまたは低い。すなわち、処理あたりのすべての負担される費用が、ネットワークの実現化に対するより高い利益マージンを与える現在の標準と等しいかまたは低い。完全に実現化戦略と共に含まれる工業および社会問題の詳細な分析を必要とする項目を別として、以下のこのテクノロジーの原理の使用は、上記リストを、項目上でさえも、良好に達成することができる。

【0290】

図2 2ないし2 6は、従く書かれた材料と共に、図2 6において「詐欺を無視しうるキャッシュカードシステム」と呼ばれるものを共に要約している。このシステムの詐欺防止特徴が、タイトルにおいて強調されている理由は、その詐欺および付随する損失取返しが、今日のプラスチックカードを基礎とする経済において中心的問題であることである。現在のシステムに対するこのシステムの差別的な利点および欠点を後に考察し、説明的な実施形態を与える。

【0291】

図2 2は、各々そして全てのユーザに対して固有の基本的偽造不可能プラスチックカードを説明する。デジタル画像9 4 0は、カードのユーザを撮ったものである。図2 6に示す中央会計ネットワーク9 8 0内に接続されたコンピュータは、デジタル画像9 4 0を受け、(図2 4を取り巻いて説明するような)その処理の後、次にパーソナルキャッシュカード9 5 0に印刷される最終的なレンドリングされた画像を発生する。さらに図2 2に示すものは、この場合においてバーコード9 5 2である簡単な識別マーキングと、図2 3に示す読み取り装置9 5 8における走査許容差を単純化するための補助することができる任意の位置基準とである。

【0292】

短い話は、パーソナルキャッシュカード9 5 0は、その個々のカードに固有の極めて大量の情報を実際に含むことである。はめ込まれた磁気ノイズ信号のような同じ原理を磁気ストリップに実際に用いることができるとしても、磁気ストリップは含まれない(クレジットカードにおける磁気ストリップの「指紋」における以前の考察を参照されたい。ここでは、指紋は、受け身に対して目立ち、予防的である。)。なんらかのイベントにおいて、パーソナルキャッシュカード9 5 0における画像内の固有情報を、基本会計情報と共に図2 6の中央会計ネットワーク9 8 0に格納する。破ることのできないセキュリティの基本は、処理中、中央ネットワークが、カードにおいて含まれる全体の情報の小さな割合を疑うことのみを必要とし、どのような2つの処理における同じ正確な情報も疑う必要がないことである。数千または数千の内の数千でないとしても数百の固有で保障された「処理証拠」が、一枚のパーソナルキャッシュカードに含まれる。暗号化された、または暗号化されていない処理の伝送に干渉しようとする著作権侵害志望者は、その後、情報に役立たないことを見つける。これは、その全体において、繰り返してアクセスすることを必要とする1つの装置で完全な(一般的に暗号化された)「キー」を有するシステムとは違うものである。他方でパーソナルキャッシュカードは、一度、数ミリ秒内で使用することができ、その後(いわば)放棄される数千の別個の保障されたキーを含む。中央ネットワーク9 8 0は、前記キーの痕跡を保持し、すでに使用されており、有していないことを知る。

【0293】

図2 3は、それらしく見えるかもしれない、代表的な売り点読み取り装置9 5 8を示す。明らかに、このような装置は、現在のキャッシュレジスタシステム、ATMシステムおよびクレジットカードの磁気ストライプ読み取り装置と、コストにおいて同等にまたは安価に製造可能である必要がある。光学的走査、画像処理およびデータ通信部品の内蔵は、図2 3において示しておらず、これらは、今後説明すべきものであり、恐らく当業者の能力内である機能を実行する通常の工学的設計方法に準じてのものである。読み取り装置9 5 8は、(一般的に、物理的なカードの盗難が発生した後)セキュリティのもう1つの信頼的レイヤを追加する通常のパーソナル識別番号システムをこのシステムの全体的な設計に結合することを示す数字タナバード9 6 2を有する。ユーザの専断の使用が、盗んだ後の不正使用を防ぐための強力な(かつ追加的に一般的に)セキュリティ特徴であることも指摘すべきであろう。カードの物理的特徴は、走査利用のセンタリング機構として重なる光学的ウィンドウ9 6 0のような機能的要素を示す。恐らく、所有者の中央商業コンピュータシステムが、可能なら中央ネットワーク9 8 0に直接接続されたデータリンクケーブル9 6 6も示す。このような読み取り装置を、購入された項目の通常の計算を行うキ

ャッシュレジスタに直接接続してもよい。カードの未加工の走査のような非電子信号がユニットから演出するかもしれないような、フラッシュメモリの形式のような読み取り装置958の構成は、ひととするとセキュリティにおいて過剰である。読み取り装置958は、後に説明するドット精査算の高速の計算において補助するデジタル信号処理ユニットを容易には含む必要がある。図25とその考察において解説した“認識”ステップにおいて使用される多数の空間パターン（直交パターン）を格納する局所的読み出し専用メモリも含むべきである。図23に示すように、プラスチックカードを使用する消費者は、単に、彼らのカードを前記ウィンドウの上に置き、商取引に関して支払う。ユーザは、彼ら自身に関して、PIN番号を使用したいかどうかを選択することができる。図25の信号処理ステップが、効果的に並列デジタル処理ハードウェアによって満たされる特性の場合、購入の許可は、おそらく数秒以内に起こる。

【0294】

図24は、ユーザの未加工デジタル画像940を、より有用な情報内容および固有性を有する画像に処理する1つの方法における大まかな様子を取り上げる。事実上、未加工デジタル画像それ自体を以下の方法において使用することができるが、追加の直交パターンの該画像への配置は、システム全体をかなり増加させてしまうかもしれないことを、明らかに指摘すべきである。（直交は、所定のパターンを他の直交パターンによって乗算した場合、結果として得られる数がゼロになることを意味し、ここで、“パターンの乗算”は、ベクトルドット積の意味であり、これらはすべて、デジタル画像処理の技術においてよく知られている言葉および概念である。）図24は、コンピュータ942が、未加工画像970の質問の後、未加工画像970に付加することができ、実際のパーソナルキャッシュカード950に印刷される画像であるより固有の画像を発生する、マスタ雪状画像972を発生することを示す。画像における全体的な効果は、画像を“テクスチャ化”することである。キャッシュカードの場合において、マスタ雪状パターンの不可逆性は、商用画像ほど高い要求はされず、マスタ雪状画像のある程度より明るく保つ唯一の規程は、ユーザの画像を曖昧にしないことである。中央ネットワーク980は、最終的な処理された画像をユーザの口座の記録に格納し、この固有で安全に保持された画像を、高度に保障された“破棄画取引キー”のキャリアとする。したがってこの画像は、ネットワーク全体におけるすべての適切な接続された売り点の場所に対して“利用可能になる”。理解されるように、売り点場所は、この画像の知識を持たず、単に、中央ネットワークからの質問に答える。

【0295】

図25は、代表的な商取引の順序を進む。この図を、第1の段が売り点読み取り装置958によって行われるステップであり、第2の段がデータライン966上で通信される情報伝送ステップを有し、第3の段がユーザの口座およびユーザの固有パーソナルキャッシュカード950についての保障された情報を有する中央ネットワーク980によって行われるステップである。字がかりによって並べ、このようなシステムの工業的実現化において通常に行われるため、これらのステップの実現化においていくらかの一致する可能性が存在するが、これらのステップをイベントの一般的な直線的順序に従って並べた。

【0296】

図25のステップ1は、光学的ウィンドウ内のパーソナルキャッシュカード950の標準的な“走査”である。これを、前記ウィンドウを走査する線形光センサを使用して、または、CCDのような2次元光検出器アレイによって行うことができる。結果として得られる走査を、アレイスケール画像にデジタル化し、光学的画像化システムの設計において一般的であるような、“フレームグラブ”のような画像フレームメモリバッファに格納する。一度カードが走査されると、第1画像処理ステップが、恐らく、4つの基準中心点954を位置決めし、これらの4つの点をすべてのさらなる画像処理動作をガイドするために使用する（すなわち、前記1つの中心は、パーソナルキャッシュカードにおける対応するパターンおよびバーコードを“正しく輸入する”）。次に、バーコードID番号を、一般のバーコード読み取り画像処理方法を使用して抽出する。一般的に、ユーザの口座番

号は、このステップにおいて決定される。

【0297】

図25のステップ2は、P I N番号の任意の印刷である。恐らく、このようなことを覚えている人間がないユーザや、誰も彼らのキャッシュカードを盗まないと確信しているユーザを除く大部分のユーザは、この特徴を有することを選択するであろう。

【0298】

図25のステップ3は、データラインを経て中央ネットワークに接続し、最新の通信ネットワークにおいて一般的な通常の通信ハンドシェイクを使用することを行う。このシステムのより洗練された実施形態は、光ファイバデータリンクのユーザのように、標準的な電話線の必要性を取り除くが、ここで我々は、既の種々のベルトーン電話を仮定し、読み取り装置958が中央ネットワークの電話番号を忘れないと仮定することができる。

【0299】

基本的な通信が確立した後、ステップ4は、売り点位置がステップ1で見つけたI D番号を、恐らく、P I N番号の（セキュリティを増すために、より確固たるRSA暗号化方法を使用するように）暗号化したものと共に送信し、売り点読み取り器958を操作する商人における基本情報と、通貨単位における必要な商取引の量とを付加する。

【0300】

ステップ5は、中央ネットワークが、I D番号を読み取り、ユーザ口座の実際のメモリ位置に従って情報をルーティングし、その後、P I N番号を照合し、口座残高が前記商取引に支払うために十分であることを検査することを行う。この方向に沿って、中央ネットワークは、商人の口座にもアクセスし、有効であることを検査し、予測されるクレジットの準備をする。

【0301】

ステップ6は、ステップ5がすべての計算を通過したという仮定によって開始するステップ6が通過していない場合の、非承認を承認に送る出口ステップは図示しない。すべてを確かめた場合、中央ネットワークは、16の番号の24の組を発生し、これらのすべての番号は相互排他的であり、一般的に、大きい方が、明確に有数の番号の範囲が存在し、そこから選択する。図25は、64Kまたは65536数である範囲を示す。実際には、どのような実際の番号とすることもできる。したがって、24の組のある組は、例えば、番号23199、51412、11007、2854、61932、32879、38128、48107、65192、522、55723、27833、19284、39970、19307および41090を有してもよい。次の組を同様にランダムにするが、前記ある組の番号をここでは前記24の組を通じて立入禁止とする。したがって、中央ネットワークは、 $(16 \times 24 \times 4 \text{ バイト})$ の番号すなわち768バイトを送る。番号の実際の量は、セキュリティ対通信速度問題の工業的最適化によって決定される。これらのランダム番号は、実際には、中央ネットワークにとって既知であり、売り点読み取り器のすべてにおけるメモリに不変に格納されている64Kの一般的に先天的に限定されている直交パターンに対するインデックスである。理解されるように、盗人志望者のこれらのパターンの知識は、役に立たない。

【0302】

ステップ7は、次に、基本的な“先に進む承認”メッセージを読み取り器958に送信し、16のランダムインデックス番号の24の組も送る。

【0303】

ステップ8は、前記読み取り器が、すべてのこれらの番号を受信し、格納することを行う。次に、前記読み取り器は、その局所的マイクロプロセッサと、注文設計された高速デジタル信号処理回路網を使用し、中央ネットワークがカードの真像の真実性を試験する“1回き”として中央ネットワークに送り返される24の別個の浮動小数点を算出する意図と共に、すべての番号の24の組を通じて両方、前記読み取り器は、これを、最終に、所定の組の16のランダム番号により示された16のパターンを合計し、次に、結果として得られた複合パターンと、カードの操作された真像との通常のドット積演算を行う。こ

のドット幅は、（簡単に、我々が浮動小数点数と呼ぶことができる）1つの数を生ずる。前記読み取り装置は、すべての24の組を通して同様に進み、24の浮動小数点数の固有の列を生ずる。

【0304】

ステップ9は、次に、前記読み取り装置が、これらの結果を前記中央ネットワークに返すことを行う。

【0305】

ステップ10は、次に、前記中央ネットワークが、これらの帰ってきた24の数において検査を行い、恐らく、それ自体正確に同じ計算を、中央ネットワークがそれ自体のメモリに有する前記カードの格納された画像に行う。再度スケール問題を取り除くために、前記読み取り装置によって送られた数を、集められた24のドット幅の最も高い絶対値をそれ自体（その無符号値）によって割ることができることを意味する“規格化”することができる。前記戻ってきた数と、中央ネットワークの計算値との結果として得られる一致は、所定の許容率内で、カードが有効である場合に満足し、カードが偽物である場合か、カードが未加工複製である場合、外れる。

【0306】

ステップ11は、次に、前記中央ネットワークが、商取引が承認されたかどうかのワードを送り、客に、彼らの購入したものと一緒に家に帰れることを知らせることを行う。

【0307】

ステップ12は、次に、商人の口座に商取引額をどのように記入するかを明瞭に示す。

【0308】

上述したように、このプラスチックカードの第1の利点は、明らかに現在のシステムに対する高い費用である詐欺を大幅に減少させることである。このシステムは、物理的カードが盗まれるか、極めて注意深く複製された場合に対してのみ詐欺の可能性を減少させる。これらの場合の双方において、PINセキュリティおよびユーザ写真セキュリティ（低い資金の事務員が署名を分析するよりも高いセキュリティの既組のシステム）が依然として残っている。カードを複製する試みは、カードの“一時的な窃盗”によって行われるとはずであり、写真品質の複製装置と、単純でない磁気カード磁気ストライプ読み取り装置とを必要とする。このシステムは、最近の24時間高度リンク化データネットワークに基づいている。商取引の不正な監視は、商取引が暗号化されているかどうかを部分的に使用しない監視を行う。

【0309】

クレジットおよびデビットカードシステムを含む商取引のセキュリティを増す前述のプロローは、いかなる写真を基礎とする識別システムにも容易に拡張されることは、明らかであろう。さらに、本技術ノロジーの原理を、写真ID文書の変化の検出と、このようなシステムの信頼性およびセキュリティの一般的な増大に用いることもできる。この関係において、例えば、パスポート、ビザ、永住許可証（グリーンカード）、運転免許証、公務員身分証明書、または民間企業身分証明バッジとすることができる。写真IDカードまたは文書1000を示す、図28を参照する。便利のため、このような写真を基礎とする身分証明文書を、総体的に写真ID文書と呼ぶ。

【0310】

写真ID文書は、文書1000にはりつけられた写真1010を含む。印刷された人間が認める情報1012が、文書1000において写真1010に近接して含まれる。“バーコード”として既知のような機械が認める情報を、前記写真に近接して含んでもよい。

【0311】

一般的に、写真ID文書を、文書の偽造（例えば、オリジナルの写真を他の写真と交換する）は、カードに顕著な損傷を引き起こすであろう。それにもかかわらず、熟練した偽造者は、存在する文書または不正製造写真ID文書を、検出することが極めて困難な方法において交換することができる。

【0312】

上述したように、本テクノロジーは、写真１Ｄ文書の使用に関するセキュリティを、写真画像に符号化情報（この情報を複眼的に感知可能にしてもなくてもよい）に付加し、それによって、文書１０００に現れる印刷された情報１０１２のような、人物に関する他の情報により写真画像の訂正を容易にすることによって拡大する。

【0313】

ある実施形態において、写真１０１０を、図２２～２４に関連して上述したようなマスク電圧画像を付加した未加工デジタル画像から発生してもよい。上述した中央ネットワークおよび読み取り装置（本実施形態においてこの装置を、入場点またはセキュリティポイント写真１Ｄ読み取り装置と考えることができる）は、本質的に、規定された直交パターンの組に対するインデックスとして動く固有番号の中央ネットワーク発生と、読み取り装置によって行われる関係するドット積演算と、中央ネットワークによって行われる同様の演算との比較を含む前記実施形態と同じ処理を行う。この実施形態において、読み取り装置および中央ネットワークによって行われるドット積演算から発生した数が一致する場合、ネットワークは、読み取り装置に、正当すなわち交換されていない写真１Ｄ文書を示す承認を送る。

【0314】

他の実施形態において、身分証明文書１０００の写真部分１０１０を、写真１Ｄ文書に組み込まれた写真画像が上記で規定したような“配布可能信号”に対応するように、デジタル化し、処理してもよい。したがって、この場合において、前記写真は、見る人には感知できず、Ｎビット識別コードを輸送する。複合理の読み取り信号を含む。この識別コードを、前記写真から、上述した復号化技術のいずれかを使用して、または、要求されるセキュリティのレベルに応じて万能またはカスタムコードを用いることによって抽出できることは、明らかであろう。

【0315】

前記写真に埋め込まれた情報が、前記文書において現れ読むことができる情報１０１２と相互に関係してもよく、余計な部分であってもよいことは、明らかであろう。したがって、このような文書を、写真１Ｄ文書を、パスポートまたはビザ管理点において利用可能なような走査システムにおいて置くことによって認証することができる。識別情報を抽出する万能コードを与えるローカルコンピュータは、オペレータが、前記符号化情報と、前記文書において輸送された読むことができる情報１０１２との相関関係を確認できるように、抽出された情報をローカルコンピュータ画面に表示する。

【0316】

写真に埋め込まれた情報は、身分証明文書における他の情報と関係する必要がないことは明らかであろう。例えば、前記走査システムは、ユーザに前記写真が偽造されているかどうかの“行け”または“行くな”情報を与えるために、前記識別コードの存在を確認することのみを必要としてもよい。暗号化デジタル通信ラインを使用するローカルコンピュータが、情報を中央証明設備に送り、その後、暗号化した“行け”または“行くな”指示を戻してもよいことも明らかであろう。

【0317】

他の実施形態において、写真に埋め込まれた識別コードを、カード運搬人の指紋のような生物測定学的データの強固なデジタル画像とし、この画像を、走査および表示後、この点における指紋認識システム（または、顔面走査、等）を用いる極めて高いセキュリティ点において、前記運搬人の実顔の指紋との比較に使用してもよい。

【0318】

写真に埋め込まれた情報は、複眼的に隠れている。または、ステガノグラフィに埋め込まれている必要はないことは明らかであろう。例えば、識別カードに組み込まれている写真を、個々の１または２次元バーコードの画像の組み合わせとしてもよい。このバーコード情報は、前記コードから得られる情報を、例えば、前記身分証明文書に印刷された情報と比較することができるようにするための、個別的な光学的走査技術（内部クロスチェックを含む）に属するものである。

【0319】

現在使用している1D文書の写事を、その能が写事において現れる個人に関連する情報を移め込むことができるように処理してもよいことも考えられる。この関係において、読み手の注意は、“全体的に埋め込まれたコードを付けることができる、印刷、紙、文書、プラスチックコーティング裏面カード、および他の材料”と表題のついたこの説明の最後の部分に向けられ、ここでは、本テクノロジーの原理の用途に従う“信号”として扱うことができる物理的媒体の変調に対する多数のアプローチが説明されている。

【0320】

固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク化方法

図27の図は、固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク化方法を与える本テクノロジーの態様を説明する。ある意味において、この態様は、ネットワークナビゲーションシステムであり、より広く、アドレスおよびインデックスをデータオブジェクトそれら自体に直接埋め込む、増強に分割されたインデックス化システムである。気付くように、この態様は、ワールドワイドウェブ(WWW)において与えられるページとのホットリンクを確立することに、特に良好に適合する。所定のデータオブジェクトは、グラフィカル表現および埋め込まれたURLアドレスの双方を有効に含む。

【0321】

先の実施形態におけるように、この埋め込みを、付加されたアドレス情報がオブジェクトの重要な値に製作者および読者に関する限り影響を及ぼさないように行う。このような埋め込みの結果として、従来のWWWリンクに伴う2つのクラス(データオブジェクトおよび別個のヘッダファイル)よりも、データオブジェクトの1つのクラスのみが存在する。ホットリンクされたデータオブジェクトが1つのクラスに載る利点を上述しており、さらに以下に詳細に説明する。本テクノロジーのある実施形態において、ワールドワイドウェブを、以前から存在するネットワークを基礎とするホットリンクとして使用する。このシステムの一般的な装置は、ネットワーク化されたコンピュータや、ウェブに接続されたときの相互作用の結果を表示するコンピュータモニタである。本テクノロジーのこの実施形態は、ウェブサイト訪問者に与えられ、“クレイスール”または“連続トーン”または“ほかし”と、結果として生じる固有ノイズとを有する画像、ビデオ、オーディオおよび他の形態のデータオブジェクトに直接ステガノグラフィに埋め込まれたURLまたは他のアドレス形式情報を考察する。上述したように、基本的なステガノグラフィの実現化を実現する種々の方法が存在し、これらのすべてを、本テクノロジーに従って用いることができる。

【0322】

図27を特に参照して、画像、疑似連続トングラフィックス、マルチメディアビデオおよびオーディオデータが、現在、ワールドワイドウェブにおける多くのサイト1002、1004の基本構成ブロックである。このようなデータを、今後、具体的に創造データファイルまたはデータオブジェクトと呼ぶ。説明する目的のため、連続トングラフィックスデータオブジェクト1006(背景を伴うタイマンリンク)を図27に示す。

【0323】

ウェブサイトツール、ウェブサイトを開発するもの1008と、これらを開発するもの1010の双方は、種々のファイルフォーマット間時に処理し、これらのデータオブジェクトをパッケージ化する。しばしば、創造者側の、これらのオブジェクトによって表される製品を売り、または創造的サービスを広告する(例えば、写真家の技術およびサービスを宣伝する、800電話番号を表示した新聞の写真)希望により、これらのデータオブジェクト1006をできるかぎり広範囲に配布することは、既に一般的である。このテクノロジーの方法を使用することにより、このようなデータオブジェクトを創造し、広める個人および組織は、ネットワークにおける彼ら自身のノート、WWWにおける彼ら自身のサイトに正しく述べて導くアドレスリンクを埋め込むことができる。

【0324】

あるサイト1004におけるユーザは、単に、表示されたオブジェクト1006において、指し示し、クリックすることを必要とする。ソフトウェア1010は、オブジェクトをホットリンクオブジェクトとして確認する。前記ソフトウェアは、そのオブジェクトに埋め込まれたURLアドレスを読み取り、ユーザが慣例的なウェブリンクを使用しているかのように、ユーザをリンクされたウェブサイト1002に送る。そのリンクされたサイト1002を、オブジェクト1006の創造者のホームページまたはネットワークノードとし、その創造者を製造者としてもよい。第1サイト1004におけるユーザに、次に、例えば、オブジェクト1006によって表される製品を購入するための注文用紙を与える

【0325】

URLアドレスまたはインデックスを埋め込まれたオブジェクト1006（これらのオブジェクトを“ホットオブジェクト”と呼んでもよい）の創造者と、彼らの品物およびサービスを宣伝することを希望する製造者とは、彼らの創作的内容を、WWWを渡る風のなかのたんぽろの種のように伝播させることができ、これらの種に埋め込まれているものが彼ら自身のホームページに上るリンクであることを知ることは明らかであろう。

【0326】

オブジェクト1006が、グラフィックの一部として組み込まれる（図27に示す好例の“H0”略語のような）明白なアイコン1012を含んでもよいことも考えられる。アイコンまたは他の微細なしるしは、オブジェクトが、埋め込まれたURLアドレス、またはソフトウェア1010によってアクセス可能な他の情報を精送するホットオブジェクトであることをユーザに知らせる。

【0327】

なんらかの人間が通知しうるしるし（例えば、短い音）は、ホットオブジェクトのユーザに知らせる目的を果たすことができる。しかしながら、このようなしるしが必要ないことも考えられる。ユーザの、アドレスが埋め込まれていないデータオブジェクトにおいてクリックする試行錯誤のアプローチは、単に、ソフトウェアがURLアドレスを捜すが見つからないことに基づくであろう。

【0328】

本テクノロジーのこの態様の使用における固有の自動処理は、極めて有利である。ウェブソフトウェアおよびウェブサイト開発ツールは、単に、これらにおいてリアルタイムに動作する、埋め込まれたホットリンク（ホットオブジェクト）のこの新たなクラスを認識する必要がある。慣例的なホットリンクを、ホットオブジェクトをウェブサイト階層内に“アップロード”することにより、グラフィックの監視以外のことを行うためのウェブサイトプログラムを必要とすることなく、簡単に変更および付加することができる。

【0329】

本テクノロジーの上述した機能を実現する方法は、一般的に、URLをステガノグラフィ的に画像、ビデオ、オーディオ、およびデータオブジェクトの他の形態に埋め込む基準の組を形成するステップ（1）と、この新たな形式のデータオブジェクト（ホットオブジェクト）を認識するようなウェブサイト開発ツールおよびウェブソフトウェアを設計するステップ（2）とを含み、前記ツールを、オブジェクトがユーザに与えられ、ユーザがこのようなオブジェクトを指し示し、クリックした場合、ユーザのソフトウェアが、どのようなステガノグラフィ的情報を読み取るまたは復号化し、ユーザを復号化されたURLアドレスに送るかを知らうに設計する。

【0330】

ステガノグラフィ的実現化を詳細に説明した本明細書の前の部分（一般的に、図2およびそれに関連する文を参照されたい）は、本テクノロジーの実現に容易に適合する。これに関して、別の慣例的なサイト開発ツール1008を拡張し、例えば、読みコード（例えば、URLアドレス）を有するビットマップ化画像ファイルを、本テクノロジーに従って符号化する能力を含むようにする。本実施形態において、商用または商取引を基礎とする

ホットオブジェクトに、上述した万能コードのいずれかを使用して、URLアドレス（または他の情報）をステガノグラフィ的に埋め込むことができる。

【0331】

ステガノグラフィ的に埋め込まれた情報を読み取るまたは復号化する技術の詳細に説明した本明細書の前の部分（一般的に、図3およびそれに関連する文を参照されたい）は、本テクノロジの実現に容易に適合する。これに関して、別の機能的なユーザソフトウェア1010を拡張し、例えば、符号化ビットマップ化ファイルを分析し、識別情報（例えば、URLアドレス）を抽出する能力を含むようにする。

【0332】

情報をデータオブジェクトにステガノグラフィ的に埋め込む説明的な実施形態を説明したが、当業者には、多数の利用可能なステガノグラフィ的技術のいずれをも、本実施形態の機能を実行するために使用することができることが明らかであろう。

【0333】

本実施形態が、WWWのいくつかの基礎構成ブロック、すなわち、画像および音を他のウェブサイトに対するホットリンクにすることができる。直接かつ一般的な意味の機構を与えることは明らかであろう。また、このようなホットオブジェクトのプロگرامmingは、単に、画像およびオーディオの配布および利用度によって完全に自動化することができる。実際のウェブサイトプログラマは必要ない。本実施形態は、非プログラマが彼らのメッセージを、単に創造的内容（ここでは、ホットオブジェクト）を形成し、配布することによって、容易に広めることができるような、WWWの商用使用を可能にする。示したように、ウェブを基礎とするホットリンクそれら自体を、より秘密のテキストを基礎とするインタフェースから、より自然な画像を基礎とするインタフェースまで取り扱うことができる。

【0334】

カプセル化ホットリンクファイルフォーマット

上述したように、一度、ホットリンクナビゲーションのステガノグラフィ的方法を理解すると、新たなファイルフォーマットおよび送信プロトコル開発として、“ヘッダを基礎とする”情報付加のより伝統的な方法が、ステガノグラフィを基礎とするシステムによって構築される基本的なアプローチを強調することができる。ステガノグラフィを基礎とするホットリンク方法をより伝統的なヘッダを基礎とする方法に拡張しはじめのある方法は、ネットワークナビゲーションシステムにおいて使用される標準的なクラスに有効になることができるファイルフォーマットの新たなクラスを規定することである。画像、オーディオ、等を越えるオブジェクトが、テキストファイル、インデックス化グラフィックファイル、コンピュータグラフィック、等を含む“ホットオブジェクト”になることができることが分かるであろう。

【0335】

カプセル化ホットリンク（EHL）ファイルフォーマットは、簡単に、予め存在するファイルフォーマットの大きな範囲の周囲に配置された小さな殻である。EHLヘッダ情報は、何らかの種類の業界標準フォーマットにおける完全に正確なファイルが動く、ファイルの最初のNバイトのみを取り上げる。EHLスーパーヘッダは、単に、正しいファイル形式と、URLアドレス、またはそのオブジェクトに関連する他の情報とを、ネットワークにおける他のノード、またはネットワークにおける他のデータベースに付加する。

【0336】

EHLフォーマットを、ステガノグラフィ的方法をゆくりと置き換える（が、恐らく完全にはない）方法とすることができる。このゆくりさきは、ファイルフォーマット標準が、しばしば、形成し、実装化し、みんなが実際にしようとするのに（するとしても）極めて長くかかるといったアイデアに敬意を払っている。再び、このアイデアは、その周囲に構築されたEHL標準フォーマットおよびシステムが、ステガノグラフィ的方法を基礎とするシステム機構に自分であることである。

【0337】

自己抽出ウェブオブジェクト

一般的に言って、データの3つのクラス、すなわち、番号（例えば、バイナリに符号化されたシリアルまたは識別番号）、英数字メッセージ（例えば、ASCIIまたは減少ビットコードにおいて符号化された人間が読むことができる名前または電話番号）またはコンピュータ命令（例えば、JAVAまたは広範囲なHTML命令）をオブジェクトにステガノグラフィ的に埋め込むことができる。埋め込まれたURLおよび上述したようなものは、この第3のクラスを覆しはじめるが、可能性のより詳細な説明を附けとすることができる。

【0338】

図27Aに示す代表的なウェブページを考える。3つの基本的な部品、すなわち、画像（#1-#6）、テキストおよびレイアウトとして見てよい。

【0339】

本願人のテクノロジを、この情報を自己抽出オブジェクトに統合し、このオブジェクトからウェブページを再発生するのに使用することができる。

【0340】

この例によれば、図27Bは、1つのRGBモザイク化画像に共に適合した図27Aのウェブページの画像を示す。ユーザは、アドビのフォショソフトウェアのような存在する画像処理プログラムを手動で利用してこの操作を行うことができ、またはこの操作を、適切なソフトウェアプログラムによって自動化することができる。

【0341】

図27Bのモザイクにおけるいくつかの画像タイルの間に、空き領域（斜線によって示す）がある。

【0342】

次にこのモザイク化画像を、ステガノグラフィ的に符号化し、レイアウト命令（例えば、HTML）およびウェブページテキストをその中に埋め込む。前記空き領域において、横ならぬ画像データが無いので、符号化デザインを最大にすることができる。次に、符号化され、モザイク化された画像をJPEG圧縮し、自己抽出ウェブページオブジェクトを形成する。

【0343】

これらのオブジェクトを、どのような他のJPEG画像としても交換することができる。JPEGファイルを開いた場合、適切にプログラムされたコンピュータは、埋め込まれた情報の存在を検出することができ、前記レイアウトデータおよびテキストを抽出することができる。他の情報と共に、レイアウトデータは、モザイクを形成する画像を最終的なウェブページにおいて配置すべき場所を特定する。コンピュータは、埋め込まれたHTML命令に従い、グラフィックス、テキスト、および他のURLへのリンクをすべて見ると、オリジナルのウェブページを形成することができる。

【0344】

前記自己抽出ウェブページを個別的なJPEGビューワーによって見た場合、自己抽出は行われない。しかしながら、ユーザは、（いくつかの画像間にノイズ様“縺”を伴う）ウェブページに関連するロゴおよびアートワークを見るであろう。当業者は、これは、代表的に、完全に抽出されない限り全体的に不明瞭に見える。他の圧縮されたデータオブジェクト（例えば、PKZIPファイルおよび自己抽出テキストアーカイブ）を見ることに全く相違していることを認識するであろう。

【0345】

（上記明点を、前記ウェブページテキストおよびレイアウト命令をJPEG圧縮モザイク化画像ファイルに関連するヘッダファイルに配置することによって、十分に達成することができる。しかしながら、このようなシステムを形成するために必要なヘッダフォーマットの業界標準は、実質的に、不可能でなくとも、困難だと思われる。）

【0346】

ステガノグラフィ的に埋め込まれた画像のパレット

URL情報を埋め込まれたウェブ画像を一旦普及すると、このようなウェブ画像を、“バレット”に転換することができ、ユーザに高いレベルのビジュアル・シミュレーションとして与えることができる。ナビゲーション系、文字通りのウェブページ・ビューアにおけるクリックよりも、このような画像（例えば、異なったウェブページのロゴ）におけるクリックによって作用される。適切にプログラムされたコンピュータは、盗取された画像から埋め込まれたURL情報を復号化することができ、要求された接続を確立することができる。

[0347]

ソフトウェアプログラムの保護および複製における本テク・ノロジーの可能な使用

ソフトウェアプログラムの不正使用、複製および転売は、ソフトウェア産業全体に対する収入の莫大の損失を意味する。この問題を軽減しようとする先行技術の方法は、極めて一般的であり、ここでは説明しない。説明することは、このテク・ノロジーの原理を、この莫大の問題にどのように関係させるかである。このテク・ノロジーによって与えられるツールが、場所および意図の双方において存在する対策を上回る何らかの経済的利点（考えられるすべてのこと）を有するかどうかは、全く明らかではない。

[0348]

最近の10年またはそれ以上に渡るテク・ノロジーの状況は、プログラムをユーザのコンピュータにおいて機能させるために、ソフトウェアプログラムの完全なコピーを直す必要を作った。実際は、SXは、Xが大きい場合、ソフトウェアプログラムの形成において使用され、その開発の全体の成果は、その全体において、ユーザがソフトウェアプログラムから価値を得るために、ユーザに渡されなければならない。幸いにも、これは一般的にコンパイルされたコードであるが、これが抽象的に見られる不確実な配布状況であることが明瞭である。この世の大部分の（および大部分の犯罪者の精神において無害な）プログラムの不正コピーおよび使用を、ある程度容易に行うことができる。

[0349]

この開示は、最初に、最も広い意味において経済的である（例えば、コスト比に対して回復される収入が、大部分の競争する方法のそれを越える）ことが分かるまたは分からない抽象的アプローチを提案する。このアプローチは、プラスチッククレジットおよびデビットカードの節において既に示した方法およびアプローチにおいて拡張する。“固有パターン”の大きな組”を仮定することによる抽象的概念は、所定の制作物に固有であり、この制作物の所定の購入者に固有である。このパターンの組は、数千、そしてさらに数百万の完全に固有の“秘密キー”を実際に含み、暗号字用語を使用する。重要かつ明白に、これらのキーは、非決定論的であり、すなわち、これらは、RSAキーを基礎とするシステムによるように、個々のサブ1000またはサブ2000ビットキーから発生しない。このパターンの大きな組を、キロバイトまたはメガバイトにおいて量り、上述したように、非決定論的とする。さらに、依然として最高の抽象的レベルにおいて、これらのパターンを、標準的な技術によって暗号化し、暗号化された領域で分析することができ、ここで書記分析を、前記パターンの大きな組の小さい部分においてのみ行い、盗人・盗業者がマイクロプロセッサのマイクロコード命令を一步一步監視している監視のシナリオにおいても、この集められた情報が、有用な情報を盗人・盗業者に与えないようにする。この後者の点は、以下に簡単に説明する“先天的セキュリティ”に対比して“実現化セキュリティ”になる場合、重要である。

[0350]

例えば、比較的簡単な、すでに重要視されているRSA暗号方法に対比して、この形式のキーを基礎とするシステムの特徴的な特性は何であらうか。上述したように、この考察は、商業的な分析を使用するものではない。代わりに、我々は、異なった特性に焦点を置いている。主な材料の特徴は、実現化領域（実現化セキュリティ）ということになる。1つの例は、1つの底ビットとアラートキーの連なる局所的な使用または再使用が、暗号化領域引システムにおいて固有に深いリンクであることである。[“暗号化領域引システム”は、ここで、ソフトウェアの支払済み使用の保障が、この考察において、ソフトウェアのユーザと、ユーザにプログラムを使用させる“ファンク”との間の事実上暗号化

された通信を必要とする意味において考察されており、他の見方において見ると、電子金融取引のサービスにおける暗号化である、いわゆる安全なシステムを打つ良かしの自明ハッカーは、方式の原始的な使用の基本的なハードウェア化とセキュリティ（元々のセキュリティ）を決して離れず、人間性および人間の監視の範囲に集まるこれらの方式の実現化を鼓う。ここで、依然として画像において、それ自体は非決定論的であり、実際に破棄キーに向けてより顕著されている、より大きなキーベースの形成は、所定の保障システムのより歴史的なような実現化を“防まぬけ”しはしめる。キーの莫大な組は、これらのキーの平均保持者に理解できず、これらのキーの読取の使用（すなわち、これらのキーの“実現化”）は、これらのキーをランダムに選択することができ、その後これらを容易に破棄することができ、これらを、“盗み聞きする人”がその盗み聞きから有用な情報をなにも得ず、特に、盗み聞きする人がキーを“解読する”ことができるまでの長い時間の内に、システムにおけるその有用性が古くなってしまいうように使用することができる。

[0951]

前記抽象性を半具体的にすることにより、ソフトウェア製品をその製品の真実の購入者にのみ安全に直す1つの可能な新たなアプローチは、以下の通りである。大規模な経済的意味において、この新たな方法は、ユーザのコンピュータネットワークと、販売会社のネットワークとの間の（しばしば、標準的暗号化をする必要がない）小規模なレートのリアルタイムデジタル接続性にもっぱら基づいている。一見して、これは、良い市場の人間の誰に對してもトラブルの匂いがし、損失収入を償おうとすることによって、重要なものを不要なものと一緒にすててしまうかもしれず、あなたは、その重（最低限の分析のすべての部分）に沿って、より正当な収入を失う。この新たな方法は、1つのソフトウェアを売る会社が、それを手に入れることを望んでいる誰かに、ユーザのネットワークに局所的な記憶装置にその機能的ソフトウェアの（速度と、送信の最小化との必要性のため）99.8％程度を供給することを命令する。この“自由コアプログラム”を、完全に非機能的とし、最も狡猾なハッカーがそれを使用することができない、またはある意味において“遅コンパイル”できないように設計する。このプログラムの正当な活性化および使用を、単に命令サイクルカウントを基礎とすると共に、単にユーザのネットワークと会社のネットワークとの間の簡単な極めて低いオーバーヘッド通信を基礎として行う。製品を使用したい客は、支払金額を会社に、多数のそうするのにより方法のいずれかによって送る。前記客に、一般的な種送り方法によって、または、一般的に保障された暗号化データチャネルを経て、彼らの“固有秘密キーの莫大な鍵”を送る。我々がこの大きな組を、画像であるかのように見ている場合、この開示の他の部分において何度も考察した雪状画像のように見える。（ここで、“署名”を、他の画像に微細に配置するよりも、画質優とする。）この画像の特別な性質は、我々が“迷方もなく固有”と呼ぶものであり、多数の選択キーを含む。（“迷方もない”は、“すべてのもの”が与える数と正確に等しい、1メガバイトのランダムビット値によって可能になる組み合わせの数における簡単な数学から来ており、したがって、1メガバイトは、多くの破棄選択キーを有する多くの人に対する十分な能力である。10の2400000乗程度になる。）購入された存在が、文字通り、ツールの生産的使用であることを再強調することは重要である。このマーケティングは、この生産性のその割り当てにおいて、前使用支払計画は、周知にユーザに興味を失わせ、明らかに全体的な収入を低くするため、極めて自由であることを必要とする。

[0952]

この選択キーの大きな組を、標準的な暗号化技術を使用して、それ自体暗号化する。比較的高い“実現化セキュリティ”に関する基礎は、ここで、それ自体を証明することを開始することができる。ここでユーザは、ソフトウェア製品を買いたいとする。彼らは、前記自由コアを始動させ、この自由コアプログラムは、ユーザが彼らの固有暗号化キーの大きな組をインストールしていることを見つかる。前記コアプログラムは、会社ネットワークを呼び、通常のハンドシェイクを行う。会社ネットワークは、キーの大きな組が莫大なユーザに属することを知り、前記ビットおよびクレジットカードの箇において説明したのほとんど正確に同じ方法で、あるパターンに簡単な組において質問を送る。この質問

は、全体の小さな組のようなものであり、コアプログラムの内部の動きは、キーのすべての組を暗号解読する必要はなく、したがって、ローカルコンピュータで自体におけるマシナリ内でのキーの暗号解読されたものは存在しない。理解できるように、これは、主な関数の「書庫内の署名」を必要とせず、代わりに、多くの固有キーが重複である。コアプログラムは、特定のドット積を行うことによってキーに照準し、次にこれらのドット積を、確認のために会社のネットワークに送り返す。図2と、それに伴う確認処理における代表的な詳細に関する考察を参照されたい。一般的に暗号化された確認を送り、コアプログラムはここでそれ自体を、ある量の命令、例えば、入力されている100000文字をワード処理プログラムに与える命令を（他の100000を可能にするために送還する必要がある他の固有キーの前に）行えるようにする。この例において、購入者は、代表的に、ワードプロセッサプログラムの一人のユーザーが一年の期間内に使用する命令の数を買うことができる。ここで、この製品の購入者は、このプログラムをコピーし、それを彼らの友人および親戚たちにあげる動機を持たない。

[0353]

上記すべては、2つの簡単な問題以外は良好である。第1の問題を「クローン化問題」と呼ぶことができる。第2の問題を「ビッグブラザー問題」と呼ぶことができる。この2つの問題に対する解決法は、緊密にリンクしている。後者の問題は、最終的に、純粋に社会的問題になり、単に道具としての技術的解決法では終わらない。

[0354]

前記クローン化問題は、以下のものである。一般的に、現在一般的な著作権侵害の形式の「友人が彼らの配布CDを友人に上げる」よりも、ソフトウェアのより洗練された著作権侵害に対して現れる。狡猾なハッカー「A」は、その全体に「埋め込まれた」プログラムのシステム機構クローン化を行い、このクローンを他の機械にインストールした場合、この第2の機械は、実際に、同じお金に対して受ける価値を2倍にすることを知っている。このクローンをデジタル記憶装置に保持することによって、ハッカー「A」は、それを再販売し、そのクローンを第1の期間が過ぎた後、再インストールする必要があるだけであり、したがって、一回の支払いに対してプログラムを無期限に使用し、すなわち、彼女は、そのクローンを彼らのハッカー友達「B」に6本バッキルのビールのためにあげることができる。この問題の1つのよい解決法は、再び、ユーザーサイトと、会社授權ネットワークとの間の、ある程度良好に開発され、低コストのリアルタイムデジタル接続性を使用する。この間接接続性は、一般的に、今日存在しないが、インターネットと、デジタルバンド幅における基本的な成長を通じて、急速に成長している。「授權」の一部および一区分は、機能化プログラムが会社ネットワークとのハンドシェイクおよび確認を日常的および不定期に行う、無視しうる通信コストランダム会計機能である。平均して、プログラムの生産性サイクリの比較的小さな量を含むサイクル中にそれを行う。結果としての平均生産性サイクルは、一般的に、全体的に授權されたプログラムのクローン化プロセスの未処理の合計コストよりもかなり低い。したがって、授權プログラムがクローン化されたとしても、その同時的なクローンの有用性は厳しく制限され、販売会社の要求する価格を支払うことは、このような短い時間間隔でクローン化プロセスを繰り返すことよりも大幅にコスト効果的になる。ハッカーは、このシステムを楽しむために破壊することができ、利益のために破壊することは確実ではない。この配列に対する裏面は、プログラムがランダムに監査のために会社のネットワークを「呼び」場合、そのプログラムにおけるそのユーザーに対して割り当てられた生産性カウントが説明され、真実の支払いが受けられていない場合、会社ネットワークは、単にその確認を中止し、プログラムはもはや機能しない。我々は、ユーザーが、（恐らく、彼らが本当に支払う場合、適切になり、「あなたが支払うそれと同様のものにかき行う」）明白な贈り物でない限り、友人に「これをあげる」動機を持たない場合に反る。

[0355]

第2の問題の「ビッグブラザー」と、ユーザーのネットワークおよび会社のネットワーク間の直観的に不可思議な「授權」接続とは、上述したように、すべての種々の可能な実在

および懸念される解決法を有するべき、社会的かつ加法的問題である。最高で客観的に打ち解けることができないデジタルシグナチャー解決法によっても、依然として、そうしないことを要求する中核的指揮理論論者が存在する。これを念頭において、1つの可能な解決法は、リアルタイム確認ネットワークを処理し、調整する、主に公的または非利益命令である。1つのプログラム登録をセットアップすることである。このような存在は、ユーザーと同様に会社を有する。例えば、ソフトウェア出版業者協会のような組織は、このような試みを導入することを選択してもよい。

[0356]

この節の結末を付すると、ここで概要を述べた方法は、高度に接続された分布されたシステム、すなわち、1995年中頃に存在するより限定的で安価なインターネットを必要とすることを、再強調すべきである。未熟なデジタル通信バンド幅における成長レートも、上記システムが、最終に現れていたよりも実地的でより速くなることを主張する。(双方面TVの見通しは、世界中の数百万のサイトをリンクする高速ネットワークの見込みをもたらす)。

[0357]

このテクノロジに関連した現在の暗号化方法の使用

このテクノロジの原理のある程度の実現化が、恐らく、現在の暗号化方法を良好に使用できることを、簡単に示すべきである。問題の1つの場合は、それによって、クラフティックアーティストおよびデジタル写真家が、かれらの写真の著作権によるリアルタイム登録を行うシステムとしてもよい。マスターコード番号、または、そのある代表的な部分を、直接第三者の登録所に有利に送ってもよい。この場合において、写真家は、かれらのコードが安全に送信され、途中で盗まれていないことを知りたいであろう。この場合において、ある一般的な暗号化処理を用いてもよい。また、写真家またはミュージシャン、またはこのテクノロジのなんらかのユーザーは、より一般的になってきている電算時間スタンダードサービスを受けたいであろう。このようなサービスを、このテクノロジの原理に開示して有利に使用することができる。

[0358]

不可視署名の合法または非法法の抽出および除去における詳細

一般的に、所定の存在が暗号的データの所定の組の中に隠れた署名を認識できる場合、同じ存在は、この署名を除去するステップを行うことができる。実際に、前の状態と後の状態との差の程度を、幸いにも、極めて大きくすることができる。ある極端において、一般的に“逆コンパイル”するのが極めて困難で、経験的データにおける承認機能を行うソフトウェアプログラムを置くことができる。一般的に、このソフトウェアの同じビットを、前記署名を(極端にすることなく)“取り除く”ことに使用することはできない。他方において、ハッカーが、わざわざ、あるデータ交換システム中で使用される“公用コード”を発見し、理解する場合、そして、ハッカーが、どのように署名を認識するかを知る場合、ハッカーが署名されたデータの所定の組を読み取り、実際に除去された署名を有するデータセットを形成するのは大きなステップではない。この後者の例において、十分に興味深く、しばしば、署名が除去されたことを暴露する統計値が存在し、これらの統計値をここでは考察しない。

[0359]

署名を除去するこれらのおよび他のこのような試みを、不正試みと呼ぶことができる。署名手法の現在および過去の説明は、一般的に、犯罪活動に属するような活動を目的としており、通常、判罰および強制用語を伴うような言葉を決まりきった法律に配置してきた。恐らく、この署名テクノロジのなんらかのおよびすべての弁護士は、これらの種類の著作権保護機構の不正除去を、同じ種類のa) 創造、b) 配布、およびc) 使用することが、強制および判罰を受けることを要する犯罪であること確かめることをするであろう。他方では、このテクノロジの指針する目的は、この開示において概要を示したステップを通じて、ソフトウェアプログラムを、署名の認識がこれらの除去に、認識プロセスにおいてこれらが見つけた信号エネルギーと同じ量によって、知られた署名を反転することによ

って、容易に至ることができるように形成することができるようにすることである。この開示においてこれを指摘することによって、この署名除去動作を行うソフトウェアまたはハードウェアは、（恐らく）犯罪であるだけでなく、（恐らく）特許を受けたテクノロジーの保有者によって正しくライセンスされていない程度の違反は免れないことが明らかになる。

【0360】

署名の合法で通常の認識の場合は、簡単である。ある例において、公用署名を値重に最低限可能に形成する（すなわち、これらの強度を値重に高くする）ことができ、この方法において、配布する“校正済み補字”の形成を行うことができる。“補字”および“校正済み”は、写真業界においてかなりしばらくの間使用されており、質を著とした画像を見込みのある客に配布し、彼らがそれを評価することができるが、商業的に意味があるようには使用できないようにする。このテクノロジーの場合において、公用コードの強度の増加は、商業的価値を意図的に低下させる方法として働き、その後、題材に対する購入金額を払うことによって活性化されたハードウェアまたはソフトウェアによって、公用署名を除去する（そして可能に、公的または私的の新たな不可視追跡コードまたは署名に置き換える）ことができる。

【0361】

監視局および監視サービス

署名の簡便かつコスト効率的な認識は、このテクノロジーの原理を広く広めるための主な問題である。この開示のいくつかの部分は、種々の方法におけるこの問題を扱う。この部分は、監視ノード、監視局、および監視代理店のような存在を、本テクノロジーの原理の組織的実施の一部として形成できるとするアイデアに焦点を合わせる。このような存在を動作させるために、マスタコードの知識を必要とし、その未加工の（非暗号化かつ無変換）形態における経験的データへのアクセスを要求することができる。（オリジナルの無署名経験的データへのアクセスを有することは、よりよい分析の助けとなるが、必要ではない）。

【0362】

監視局の3つの基本的な形態は、マスタコードの明白に任意に規定されたクラスから直接引き、私的監視局、半公的および公的である。この区別は、単にマスタコードの知的を基礎としている。完全に私的監視局の一例を、特定の基本的パターンをその配布された題材中に配置することを決め、真に狡猾な個人が解説および除去することができることを知るが、この可能性は、経済的スケールにおいて馬鹿げたほど小さいと考える。大きな写真所産社としてもよい。この所産社は、高価値の広告および著作権撤消失状態の他の写真を受付、ランダムに検査し、基本的パターンを見つけるのが比較的容易なこれらを探し、その所産社の社員が、それが侵害された題材かもしれないと“認め”考えた写真を検査するバートタイマーを雇う。このバートタイマーは、数時間以内にこれらの多量の侵害された可能性のある場合を巡回し、基本パターンが見つかった場合、より徹底的な分析を行い、オリジナル画像を突き止め、この開示において開示を示したような固有識別の完全な処理を行う。2つの中心的な経済的価値が、これを行う所産社に対して生じ、定直によるこれらの価値は、監視サービスのコストおよび、署名処理自体のコストをよりもまざる。第1の価値は、彼らの客および世界が、彼らが彼らの題材に署名しており、侵害者を捕らえる能力におけるどんな統計によっても支援された監視サービスが存在することを知らせることにおけることである。これは即時的価値であり、恐らく、結局最も大きい価値であろう。この第1の価値に対して一般的な予め必要なのは、（第1の価値を推測する）恐ろしくするための、監視努力と、その追跡記録の精確にから得られた、実際に取り戻された著作権使用料である。

【0363】

半公的監視局および公的監視局は、これらのシステムにおいて、マスタコードの知識を客によって与えられた第三者のサービスを実際に始めることができ、前記サービスが、数千および数百万の“創造的価値”を通じて複製、コードを探索し、結果を客に報告すると

しても、大部分同パターンに従う。ASCAPおよびBMIは、この基本的なサービスに対する“より良い技術”のアプローチを有する。

【0364】

このテクノロジーの原理を使用する大いに関与された監視サービスは、その創造的特性供給客を2つの基本的なカテゴリに分類し、これらは、一般的に公的領域マスコード（と、もちろんこれら2つの見込物）を使用する。この監視サービスは、スーパーコンピュータのバンクによる高レベルパターン検査を行う、公的に利用可能な画像、ビデオ、オーディオ等の毎日の膨大化（検査）を行う。監視広告および画像を分析のために走査し、南州チャンネルの広まったビデオをデジタル化し、オーディオを標準化し、公的インターネットサイトをランダムにダウンロードする、等を行う。次にこれらの基本的データストリームを、その公的および私的コードの大きいバンクと、検査しているデータ題材とのパターン一致をランダムに探す常時監視監視プログラムに供給する。それ自体が恐ろしく大きな組である小さなサブセットを、一致の可能性のある候補として含括し、これらを、正確な署名が存在することを識別し、与えられた含括された題材においてより精密に分析する試みを開始する。より精密な検査システムに供給する。恐らく、次に、小さな組が、含括された一致題材ということになり、その題材のオーナーを明確に確認し、監視報告を客に送り、彼らが、彼らの題材の合法的販売であることを確認できるようにする。上記で概要を述べた私的監視サービスの同じ2つの価値は、この場合において同様に適合する。この監視サービスは、発見され、証明された侵害の場合においてフォーマットフリーとしても働き、侵害する当事者に、見つけた侵害を立証し、誇張的な著作権使用料を要求する手紙を送り、侵害する当事者が、より費用が掛かる裁判所に行く選択を回避できるようにする。

【0365】

サブミナル登録パターンを画像および他の信号に埋め込む方法

埋め込まれた信号の読み取りの概念は、登録の概念を含む。下にあるマスコード信号を知らなければならず、その関係する部分を、読み取り処理それ自体（例えば、Nビット識別ワードの1および0の読み取り）を始めるために、確定（登録）する必要がある。誰かが無署名信号のオリジナルまたはサムネイルへのアクセスを有する場合、この登録処理はまったく簡単である。誰かがこの信号へのアクセスを持たない場合、これは、しばしば、このテクノロジーの万能コード用途における場合となり、異なった方法をこの登録ステップを行うために用いる。定義により、“無署名”オリジナルには成らない。予め印が付けられた写真フィルムおよび紙の例は、後者の点における完全な場合である。

【0366】

多くの前の節は、この問題を種々に考察し、ある程度の解決法を与えた。明白に、“簡単な”万能コードにおける節は、所定のマスコードが先天的に既知であるが、その正確な場所（そして、その存在または非存在）は知られていないという解決法の実施例を考察する。この節は、極めて低いレベルの設計された信号を、極めてより大い信号内にどのように埋め込むことができるかの特定の例を与え、ここで、この設計された信号を標準化し、検出装置または読み取り処理が、この標準化信号を、その正確な場合が分からないにもかかわらず、探すことができるようにする。2D番号コードにおける短い節は、この基本概念を2次元、または実際に、画像および動画に拡張できることを指摘する。また、対称パターンおよびノイズパターンにおける節は、2次元の場合に対するさらに他のアプローチの戦略を述べ、ここで、2次元スケールおよび回転に関連するニュアンスを、より明白に述べる。その点において、前記アイデアは、下にあるノイズパターンの正確な方向およびスケールを単に決定することではなく、同様に送信される情報、例えば、Nビット識別ワードに関するうちのリンクを有することもある。

【0367】

この節は、登録のために、埋め込まれたパターンを登録するサブ問題を分離することを試みる。埋め込まれたパターンが一度登録されると、我々は、この登録が、より広い要求にどのように役に立つことができるかを見ることが出来る。この節は、パターンを埋め込むさらに他の技術と、“サブミナルデジタルグラフィック”と呼ぶことができる

技術を与える。“グラフィキユール”一基準、または、レチクル、または、ハッシュマークのような他の言葉は、なにかを位置決めおよび/またはは確定する目的に使用されるキャリブレーションマークのアイデアを伝えることに良好に使用することができる。この場合において、一種のグリッド機能として働く低レベルパターンとして使用する。そのグリッド化機能は、1秒の万端ノイズにおけるような1ビットの情報(その存在または存在、複製化、複製不可)のキャリヤとすることができ、または、埋め込まれた信号のような他の情報(方向およびスケールを単に見つけることができ、画像またはオーディオオブジェクトそれぞれを単に適合させることができる。

[0368]

図29および30は、本願のサプリミナルディジタルグラフィキユールを説明する2つの関係する方法を視覚的に要約する。考察するように、図29の方法は、図30において概要を示した方法よりむしろ実用的な利点を有するが、双方の方法は、精洗法に取次する一連のステップへの画像の進捗を見つける問題を有効に分析する。全体としての問題を、単に以下のように言うことができる。サプリミナルディジタルグラフィキユールをスタンプされているかもしれない任意の画像を与えた場合、サプリミナルディジタルグラフィキユールのスケール、回転、および原点(オフセット)を見つける。

[0369]

サプリミナルグラフィキユールに関する問題点は、これらが何であるかを規定することである。簡単に述べると、これらは、他の画像に直接付加された、または、場合に応じて、写真フィルタまたは紙上に露出した視覚的なパターンである。古典的な2重露出は、ディジタル画像化においてこの特定の概念がいくぶん拡大するとしても、悪いアナログでは無い。これらのパターンは、一般的に、これらが“通常の”画像および露出と組み合わせられた場合、実際に不可視(サプリミナル)になり、埋め込まれた署名による場合のように、定義によって、これらが付加された画像の広い値と干渉しないような、極めて低輝度レベルまたは露出レベルにおけるものである。

[0370]

図29および30は、各々、UVプレーン1000として既知の特定の周波数領域において表されるような、サプリミナルグラフィキユールの2つのクラスを規定する。一般的な2次元フーリエ変換アルゴリズムは、所定の画像をそのUVプレーン共役に変換することができる。明確にするために、図29および30における描写を、特定の周波数の振幅とするが、すべての点において存在する位相および振幅を描写することは困難である。

[0371]

図29は、45度線に沿った各々の象限における6つの点の例1002を示す。これらの点をUVプレーンの視覚的検査によって識別することは困難であるため、これらをこの図において誇張している。任意の画像の“代表的”なパワースペクトルの値(描写1004)を示す。このパワースペクトルは、一般的に、画像が独特であると同じ位相特である。サプリミナルグラフィキユールは、本質的にこれらの点である。この例において、2つの45度線の各々に沿って結合された6つの空間周波数が存在する。これら6つの周波数の振幅は、同じであっても異なってもよい(この微妙な区別については後に触れる)。一般的に言って、各々の位相は互いに異なり、他の対して45度線の位相を含む。図31は、これをグラフ式に示す。この例における位相は、1008および1010に、P1およびP1間で簡単にランダムに配置されている。反映した象限はその振幅を単にP1/2としたものであるため、4つの別個の象限に対して、2つの軸のみを図31において表す。我々が、このサプリミナルグラフィキユールにおける強度を大きくし、その結果を画像領域に変換した場合、図29の説明において述べたような波状クロスハッチパターンを見るであろう。述べたように、この波状パターンは、所定の画像に付加された場合、極めて低い強度におけるものである。使用するスペクトル成分の正確な周波数および位相を格納し、順序化する。これらは、空間線画および読み取りプロセスが求め、規定する。“スペクトル署名”になる。

[0372]

簡単に、図30は、この同じ一般的なテーマにおける変形例を有する。図30は、スペクトル周波数が、4.5度軸に沿った点よりも、同心リングの順次列になる。グラティキュールの形になったクラスを示す。図32は、縦向きランダム位相プロファイルを半周期に沿った周波数として示す(周期の他の半分は、最初の半分の位相から $P/2$ ずれている)。これらは簡単な例であり、これらの同心リングの位相プロファイルおよび半径の設計において可能な、広範囲に種々の変形例が存在する。この形式のサブミナルグラティキュールの変形は、図29の減速グラティキュールによるような“パターン”が少なく、雲状画像のようなランダムな様子が多い。

【0373】

双方の形式のグラティキュールの背後のアイデアは、以下の通りである。固有パターンを、それが付加されている画像から常に視覚的に区別されるが、パターンの高選択位置決めを容易にする特定の特性と、パターンが一般的に位置決めされた場合、その正確な場所および方向を、ある大家レベルの精密さで見つけることができるような精度特性とを有する画像に埋め込む。上記に対する結果は、パターンが、平均して、それを付加する代表的な画像と僅かにしか干渉せず、パターンの可視度に対して最大のエネルギーを有する、パターンを設計することである。

【0374】

全体的なプロセスがどのように動くかすべての要約を進むと、図29のグラティキュール形式は、サブミナルグラティキュールの回転軸を最初に位置決めすることによって始まり、次にグラティキュールのスケールを位置決めし、次に原点またはオフセットを決定する。画像処理調査を容易にする。ここで、最後のステップは、軸が2つの4.5度軸のいずれであるかを、位相を決定することによって確認する。したがって、画像が大きく混乱していても、正確な決定を行うことができる。第1のステップおよび第2のステップを、位相および振幅と対比して、パワースペクトルデータのみを使用して行うことができる。次に、位相および振幅信号を使用して、正確な回転角およびスケールの調査の“細かい調整”を行うことができる。図30のグラティキュールは、上記最初の2つのステップを切り替え、最初にスケール、次に回転を見付け、原点の正確な決定を続ける。当業者は、これらの顕著なパラメータを2つの軸に沿って決定することが、画像を完全に登録するために十分であることを、認識するであろう。“工業的最適化の挑戦”は、パターンの固有さおよび精度をこれらの可視度に対して最大にし、登録における精度のある特定のレベルに到達することにおける計算オーバーヘッドを最小にすることである。写真フィルムおよび紙を露出する場合において、明らかに、追加の工業的挑戦は、まず第1に、フィルムおよび紙上に露出したパターンを得る経済的ステップの戦略であり、この挑戦は、前の節において指摘されている。

【0375】

上記で規定した問題および解決法は、登録の目的のための登録を意図するものである。グラティキュールが実際に見つかるかどうかにかかわらずある種の詳細判断の形成によって形成される記録はないことに注意されたい。明らかに、上記ステップを、実際にその内部にグラティキュールを持たない画像に用いることができ、このとき測定は、単にノイズを追跡する。共感か、これらのパターンの形式に対する“検出しき値”を設定する仕事を割り当てられたエンジニア、または、パターンを捜し、確認する必要がある画像および関連の検出の速方もなく広い範囲の中の間隔に広がる必要がある。[反面的に、これは、純粋に万能な一歩のノイズを前の節において置いたことであり、この単一の信号を単に検出する。または検出しき値を越えていく、すなわち、追加の情報プレーンを追加することがなぜ適切なものである。] このような事情は、サブミナルグラティキュールの、この開示の他の部分において説明した登録された埋め込まれた署名との結合において、ある本当の英人が現れることである。明確に、ノイズを追跡することができるアイデアに敬意を払い、一度“志願者登録”が見つかると、次の論理ステップは、例えば、6.4ビット/行能コード署名の、読み取り処理を行うことである。他の例として、我々は、6.4ビット/識別ワードの4.4ビットを、登録されたユーザのインデックス、こういう言い方を許しても

らえるならばシリアル番号として割り当てることを想像することができる。残りの20ビットを、このように得られた44ビット識別コードにおける、暗号化技術においてよく知られている、ハッシュコードとして暗号化する。したがって、一単位は、20ビットが、“はい、私は登録された画像を持っています”または“いいえ、私は持っています”の答えとして働く。より重要に、ひょっとすると、これは、どのような自動化識別システムにおいても、“誤った肯定”のレベルを正確に規定することにおいて最高に柔軟にすることができるシステムを考慮する。しきい値を基礎とする検出は、常に、最終的に任意の決定に基づき過剰な状態および状況のなすままになるであろう。いつの日もNのコイン投げを与えてくれ。

【0376】

点に照ると、これらのグラティキュールパターンを、最初に、画像に付加するか、フィルム上に露出しなければならない。好例のプログラムは、任意のサイズのデジタル画像において読み取り、特定したグラティキュールをこのデジタル画像に付加し、出力画像を発生する。フィルムの場合において、グラティキュールパターンをフィルム上に、本来の画像の露出中または後に、物理的に露出する。これらの方法のすべては、これらをどのように行うかにおいて、広い変形例を有する。

【0377】

サブリミナルグラティキュールの探索および登録は、より興味深く、必要とされるプロセスである。この節は、最初に、このプロセスの要素を説明し、図37の一般化したフローチャートにおいて終わる。

【0378】

図33は、図29における形式のグラティキュールに対する登録プロセスの第1の主要な“探索”ステップを示す。疑わしい画像（または、疑わしい写真の走査）を、最初に、既知の2D FDFトルチンを使用して、そのフーリエ表現に変換する。入力画像は、図36の左上のもののように見える。図33は、続く処理が回転問題に完全に対処するとしても、画像およびグラティキュールが回転されていない場合を概念的に表す。疑わしい画像を変換した後、変換のワースベクトルを計算し、2つの自乗した係数の和の平方根とする。3×3ブラフフィルタのような軽いローパスフィルタ処理の結果として得られたワースベクトルデータに行い、後の探索ステップが遠方もなく細かく、道筋のステップを必要としないようになることも、良いアイデアである。次に、0ないし90度の候補回転角（または、半径において0ないし $P1/2$ ）を進める。何らかの角度に沿って、2つの結果として生じるベクトルを計算し、第1のベクトルは、各々の側面における原点から放射する4本のラインに沿った所定の角度におけるワースベクトル値の単純な足し算である。第2のベクトルは、第1のベクトルの移動平均である。次に、規格化パワープロファイルを、1.022および1.024に示すように計算し、その違いは、一方のプロットが、サブリミナルグラティキュールと整列しない角度に沿っており、他方のプロットは整列している。規格化は、第1のベクトルが結果として得られるベクトルの分母であり、第2のベクトルが分子であることを規定する。図33の1.022および1.024において分かるように、ピークの列（図示した“5”の代わりに“6”にすべき）は、角度がその本来の方向に沿って整列する場合に現れる。これらのピークの検出を、あるいは値を前記規格化値に設定し、これらの合計を半径ライン全体に沿って積分することによって行うことができる。0ないし90度のプロット1.026を図33の下部に示し、これは、角度45度が最大エネルギーを含むことを示す。実際に、この信号は、しきい値、この下部の図に示すよりもかなり低く、最高値を“見つかった回転角”として選択する代わりに、単に、少数の最高の候補角を見つけ、これらの候補を、登録を決定するプロセスの次の段階に提出することができる。前述のことが簡単に既知の信号検出計画であり、最終的に形成または借用することができる。このような多数の計画が存在する技術の当業者によって、理解することができる。第1段階のプロセスの簡単な必要なのは、候補回転角をいくつかに減らすことであり、次に、より精密な探索が引き継ぐことができる。

【0379】

図3 4は、パワースペクトル領域における同様の形式の全体的な探索の概要を本質的に述べる。ここで代わりに、我々は、回転角よりも、最初に同心リングの全体的なスケールにして、小さいスケールから大きいスケールまで進むことによって、探索する。1 0 3 2に示すグラフは、1 0 2および1 0 2 4と同じ規格化ベクトルであるが、ここでは、ベクトル値を半円に沿った角度の関数としてプロットした。前記移動平均を、依然として、接線方向よりも半径方向において計算する必要がある。プロット1 0 4 0を生じることによって理解できるように、規格化信号における同様の“ピーク化”は、走査された円が、クラテスキュール円と一致する場合に生じる。次にスケールを、下部のプロットにおいて、同心リングの既知の特徴(すなわち、これらの半径)を1 0 4 0におけるプロファイルと一致させることによって見つけることができる。

【0380】

図3 5は、図2 9における形式のサブミナルグラティキュールを登録することにおける第2の主要なステップを示す。一度、我々が図3 3の方法によっていくつかの回転候補を見つけたと、次に、我々は、1 0 2 2および1 0 2 4の形式の候補円のプロットを取り、本発明者が、これらのベクトルにおけるフィルタ処理動作に適合する“スケール化カーネル”と呼ぶことを行う。スケール化カーネルは、この場合におけるカーネルが、1 0 4 2および1 0 4 4の上部におけるxのラインとして表される既知の周波数の非調和関係であり、これらの周波数のスケールが、ある要求される1 0 0%におけるスケールの2 5%ないし4 0 0%のようなある予め決められた範囲に広げることに関連する。整合フィルタ演算は、単に、結果として生じるスケール化周波数の乗算された値と、これらのプロットの片側とを加算する。当業者は、この演算の、極めて良く知られている整合フィルタ演算との類似性を認識するであろう。整合フィルタ演算の結果として得られるプロットは、いくらか図3 5の下部における1 0 4 6のように見える。前記第1ステップからの各々の候補は、それ自身のこのようなプロットを発生し、この時点においてこれらのプロットの最高値が我々の候補スケールになる。図3 0の形式のグラティキュールと同様に、同様の“スケール化カーネル”整合フィルタ演算を、図3 4のプロット1 0 4 0において行う。これは、一般的に、1つの候補スケール係数を与える。次に、図3 2の格納された位相プロット1 0 1 2、1 0 1 4および1 0 1 6を使用して、より徹底的な整合フィルタ演算を、(カーネルとして)これらの格納されたプロットと、前に見つかったスケールにおける半周期に沿って測定された位相プロファイルとの間に用いる。

【0381】

図2 9の形式のグラティキュールの登録の最後のステップは、クラテスキュールの既知の(スペクトルまたは空間)プロファイルと、疑わしい直線との間の、普通の種々の整合フィルタ演算を行うことである。回転、スケールおよび方向が、前のステップによって分かっていることから、この整合フィルタ演算は簡単である。正確で精密な前のステップが、処理において設計仕様を越えていない場合、簡単な小規模の探索を、スケールおよび回転の2つのパラメータについて小さい領域において行うことができ、行われた整合フィルタ演算と、見つかった最高値とは、“細かく調節された”スケールおよび回転を決定する。この方法において、スケールおよび回転を、疑わしい直線それ自体のノイズおよびクロストークによって設定された程度内で見つけることができる。同様に、一度、図3 0の形式のグラティキュールのスケールおよび回転が見つかったと、簡単な整合フィルタ演算は、この登録プロセスを完了することができ、同様に、“細かい調節”を適用することができる。

【0382】

図2 9、図3 6の形式のグラティキュールの使用の変形に進むことは、計算に関して不連続な二次元FFT(高速フーリエ変換)を行う必要なく、サブミナルグラティキュールを見つける可能性を与える。計算オーバーヘッドが大きな問題である状況において、探索問題を、一度の二次元ステップに減少させることができる。図3 6は、これをどのように行うかを明白に示す。左上におけるこの図は、図2 9の形式のグラティキュールが埋め込まれた任意の画像である。0度から始め、例えば5度ずつ進み、1 8 0度で終わることに

よって、図示した列に沿ったグレイ値を単純に加算し、結果として得られる列一横分走査1058を形成することができる。この図の右に、1058とは、これを行う多くの角度の1つを示す。次にこの列一横分走査を、計算に関してあまり不経済でない一次元FFTを使用して、そのフーリエ表現に変換する。次にこれを、振幅または「パワー」プロット（これら2つは異なる）に変え、図33における1022および1024と同様の規格化ベクトルバージョンを形成する。ここでの違いは、角度がグラティキュールの正しい角度に近づくにつれ、1024のようなプロットにおいて、表示セクタがゆっくりと現れ始めるが、これらは、我々は一般的に我々の回転において僅かに外れていることから、一般的に、所定のスケールに要求されるよりも高い周波数において現れることである。ピーク信号を最大にする角度を見つけることが残っており、したがって、正しい角度においてズームインする。一度、正しい回転が見つかったと、スケール化カーネル整合フィルタ処理を行うことができ、すべて上述した慣例的な整合フィルタ処理を続ける。再び、図36の「ショートカット」の1つのアイデアは、図29における形式のグラティキュールを使用することにおける計算オーバーヘッドを大幅に減少させることである。本発明者は、たとえ実現されなくても、図36のこの方法を習慣のため減少させておらず、正確にどの位計算に関して節約できるかにおけるデータを現在持たない。これらの試みは、方法の用途を特定した発展の一部である。

【0383】

図37は、主要なプロセスステップの順序における、図29の形式のグラティキュールの間隔を回転する方法を簡単に要約する。

【0384】

他の変形実施形態において、グラティキュールエネルギーは、空間周波数領域において45度に関係しない。代わりに、このエネルギーは、より広く空間的に分布する。図29Aは、あるこのような分布を示す。軸の近傍および原点の近傍の周波数は、画像エネルギーが最も集中すると思われる場所であるため、一般的に無効になる。

【0385】

疑わしい画像におけるこのエネルギーの検出は、再び、上述したような技術を頼る。しかしながら、最初に軸を確認し、次に回転を確認し、次にスケールを確認する代わりに、すべてを暴力的試みにおいて決定する、より包括的な整合手順を行う。当業者は、フーリエ・メーン変換が、このようなパターン整合プログラムにおける使用に好適であることを認識するであろう。

【0386】

前述の原理は、例えば、写真複製キオスクにおける用途を得る。このような装置は、代表的に、客が与えたオリジナル（例えば、写真プリントまたはフィルム）を光電子検出器に結ぶレンズと、感光乳剤基板（再び、印刷紙またはフィルム）を前記検出器によって得られた画像データに従って、露出し、現像するプリント書き込み装置とを含む。このような装置の詳細は、当業者には既知であり、ここでは考察しない。

【0387】

このようなシステムにおいて、メモリは前記検出器からのデータを格納し、プロセッサ（例えば、支持部品と関係するベンチアムマイクロプロセッサ）を使用し、メモリデータを処理し、それにステガノグラフィ的に埋め込まれた著作権データの存在を検出することができる。このようなデータが検出された場合、プリント書き込みを中断する。

【0388】

オリジナル画像の軸から外れた手動の回転によるシステムの失敗を回避するために、前記プロセッサは、上述した技術を望ましく実現化し、スケール、回転および原点のオフセット因子にもかかわらず、オリジナルの自動変換を行う。もし望むなら、ディジタル信号処理ポートを使用し、メイン（例えば、ベンチアム）プロセッサによるFFT処理のある程度を取り除くことができる。回転した/スケール化した画像を登録した後、どのようなステガノグラフィ的に埋め込まれた著作権情報の検出も簡単であり、機械が写真家の著作権の侵害において使用しないことを確実にする。

【0389】

開示した技術は、本職人の好むステガノグラフィ的符号化方法の使用を行ったが、その原理を、より広く適用でき、画像の自動登録を行うべき多くの場合において使用することができる。

【0390】

ビデオデータストリームが高速一方モデムとして効率的に働く、ビデオに埋め込まれた信号の使用

以前の節において概要を述べた万能コード化システムの使用によって、そして、簡単な方法でフレーム毎に変化するマスク常流フレームの使用によって、簡単な受信機を、マスク常流フレームにおける変化の予めの知識を有し、したかつて、フレーム毎（または、MPEGビデオにおけるとしてもよい場合のように1フレーム毎）に変化するNビットメッセージワードを読み取ることができるよう設計することができる。この方法において、動画シーケンスを、一方モデムのような、高速一方情報チャネルとして使用することができる。例えば、ステガノグラフィ的に埋め込まれ、Nビットメッセージの送信を行うN本の走査ラインを有するビデオデータのフレームを考える。フレーム(N)において484走査ラインが存在し、フレームが一秒に30回変化する場合、14.4キロボードモデムに匹敵する容量を有する情報チャネルが達成される。

【0391】

実際において、フレーム当たりNビットの超過において十分なデータレートが通常達成され、1SDN回路の送信レートに近い送信レートになる。

【0392】

無線通信における詐欺防止

セルラ電話産業において、サービスの信頼により、毎年1億ドルの収入が損失する。いくつかのサービスは、セルラ電話の物理的脆弱によって損失するが、より有害な脅威がセルラ電話ハッカーによってもたらされる。セルラ電話ハッカーは、種々の電子装置を用い、許可されたセルラ電話によって発生された識別信号を模倣する。(これらの信号は、時々、許可信号、識別番号、署名データ、等と呼ばれる。)しばしば、ハッカーは、これらの信号を、許可されたセルラ電話加入者を偽り聞きし、セルサイトと交換されたデータを記録することによって学習する。このデータの巧妙な使用によって、ハッカーは、許可された加入者を真似ることができ、キャリアを騙して非合法な通話を完成することができる。

【0393】

先行技術において、識別信号を音声信号から分離する。最も一般的に、これらは、時間的に分離され、例えば、通話開始時にバーストにおいて送信される。音声データは、証明動作がこの識別データにおいて行われた後にも、チャネルを通過する(識別データを、一般的に、送信中に送られるデータパケットにも含める)。他のアプローチは、識別を、例えば、音声データに割り当てられたバンド以外のスペクトルサブバンドにおいて、スペクトル的に分離することである。

【0394】

他の詐欺防止計画も用いられている。あるクラスの技術は、セルラ電話のRF信号の特徴を監視し、源を発する電話を識別する。他のクラスの技術は、ハンドシェイクプロトコルを使用し、セルラ電話によって送られるデータのいくつかを、それに送られるランダムデータに用いられるアルゴリズム(例えば、ハッシュ化)を基礎とする。

【0395】

前述のアプローチの組み合わせも、時々用いられる。

【0396】

米国特許明細書第5,465,387号、第5,454,027号、第5,420,910号、第5,448,760号、第5,335,278号、第5,345,595号、第5,144,649号、第5,204,002号、第5,153,019号および第5,388,212号は、種々のセルラ電話システムと、そこで使用される詐欺防止技術とを評述している。これらの特許の開示は、参照によって取り入れられる。

【0397】

詐欺防止システムの信頼度が暫すにつれて、セルラ電話ハッカーの信頼度も増している。最終的に、ハッカーは、彼らが、全ての先行技術システムが同じ弱点、すなわち、識別が音声データ以外のセルラ電話送信のある属性を基礎としていることに対して働いていることを認識しているため、より優勢である。この属性は、音声データから分離されていることから、このようなシステムは、これらの音声で、詐欺防止システムを破るのに必要な属性を有する複合電子信号に、電子的に“でっち上げる”盗人に対して常に影響を受けやすい。

【0398】

この欠点を克服するために、本テクノロジーのこの態様の好適実施形態は、音声信号を識別データと共にステガノグラフィ的に符号化し、結果として、“帯域内”周波信号（時間およびスペクトルの両方において帯域内）を生じる。このアプローチは、キャリアがユーザの音声信号を監視し、そこから識別データを復元することを可能にする。

【0399】

本テクノロジーのあるこのような形態において、先行技術において使用されている識別データのいくらかまたはすべて（例えば、通話開始時に送信されるデータ）を、同様にユーザの音声信号に繰り返しステガノグラフィ的に符号化する。したがってキャリアは、音声データに伴う識別データを通話開始時に送られる識別データと周期的または非周期的に検査し、これらの一致を保証する。これらが一致しない場合、この通話を、ハックされていると認め、通話を中断するような改善のためのステップを行うことができる。

【0400】

本テクノロジーの他の形態において、いくつかの可能なメッセージのランダムに選択された1つを、電話加入者の音声に繰り返しステガノグラフィ的に符号化する。通話開始時にセルラキャリアに送られたインデックスは、期待されるメッセージを認識する。電話加入者の音声からセルラキャリアによってステガノグラフィ的に復号化されたメッセージが期待されたものと一致しない場合、この通話を不正として認識する。

【0401】

本テクノロジーのこの態様の好適な形態において、ステガノグラフィ的符号化は、疑似ランダムデータ信号を頼り、メッセージまたは識別データを、電話加入者のデジタル化された音声信号に重ねられた低レベルノイズ状態信号に変換する。この疑似ランダムデータ信号は、（符号化に関して）電話加入者の電話と、（復号化に関して）セルラキャリアとの双方に対して知られている、または知られうる、多くのこのような実施形態は、電話およびキャリアの双方に対して知られている基準の種を備わった決定論的疑似ランダム数発生器を頼っている。簡単な実施形態において、この種を、あるセルから次のセルまで一定（例えば、電話1D番号）のままとすることができる。より複雑な実施形態において、疑似一回バッドシステムを使用することができ、新たな種を各々のセッション（すなわち、通話）に対して使用する。混成システムにおいて、電話およびセルラキャリアの各々は、基準ノイズキー（例えば、10000ビット）を有し、そこから電話は、ランダムに選択されたオフセットにおいて開始する50ビットのようなビットの領域を選択し、各々がこの秩序を種として使用し、符号化のための疑似ランダムデータを発生する。通話開始中に電話からキャリアに送られたデータ（例えばオフセット）は、キャリアに、復号化に使用する同じ疑似ランダムデータを再構成させる。さらに他の改善を、基本的技術を種号通信の技術から借用し、これらをこの開示において詳述したステガノグラフィ的に埋め込まれた信号に用いることによって得ることができる。

【0402】

疑似ランダムデータストリームによるステガノグラフィ的符号化/復号化に関する本開示の先行技術の詳細は、本明細書の以前の部分においてより特に詳述されているが、このテクノロジーは、このような技術との使用に限定されない。

【0403】

読み手が、セルラ通信技術に精通しているとする。したがって、この分野における先行技術から既知の詳細を、ここでは考察しない。

【0404】

図38を参照すると、説明的なセルラシステムは、電話2010と、セルサイト2012と、中央局2014とを含む。

【0405】

概念的に、電話を、マイクロフォン2016と、A/Dコンバータ2018と、データフォーマッタ2020と、変調器2022と、RFセクション2024と、アンテナ2026と、復調器2028と、データアンフォーマッタ2030と、D/Aコンバータ2032と、スピーカ2034を含むものとして見る事ができる。

【0406】

動作において、電話加入者の音声は、マイクロフォン2016によって拾われ、A/Dコンバータ2018によってデジタル形態に変換される。データフォーマッタ2020は、ディジタル化された音声を、パケット形態にし、同期化および制御ビットを付加する。変調器2022は、このディジタルデータストリームを、位相および/または振幅が変調されているデータに従って変化するアナログ信号に変換する。RFセクション2024は、一般的に、この時間変化する信号を、1つ以上の中間周波数に変え、最終的にUHF送信周波数に変える。RFセクションは、その後、それを増幅し、結果として得られる信号を、セルサイト2012に放送するためにアンテナ2026に供給する。

【0407】

このプロセスは、受信時に逆に動く。セルサイトからの放送は、アンテナ2026によって受信される。RFセクション2024は、受信された信号を増幅し、復調のための異なる周波数に変える。復調器2028は、RFセクションから供給された信号の振幅および/または位相変化を処理し、それに対応するディジタルデータストリームを発生する。データアンフォーマッタ2030は、関係する同期化/制御データから音声データを分離し、この音声データをアナログ形態に変換するためにD/Aコンバータに渡す。D/Aコンバータからの出力は、スピーカ2034を駆動し、これを通して電話加入者は、他の関係者の音声を聞く。

【0408】

セルサイト2012は、複数の電話2020からの放送を受信し、受信されたデータを中央局2014に中継する。同様に、セルサイト2012は、中央局から出たデータを受信し、同じものを電話に放送する。

【0409】

中央局2014は、セル認証、切り替え、およびセルハンドオフを含む種々の動作を行う。

【0410】

(いくつかのシステムにおいて、セルサイトおよび中央局間の機能区分が、上記で概略述べたものと異なる。実際は、いくつかのシステムにおいて、この機能のすべては、1つのサイトにおいて与えられる)。

【0411】

本特許ノロジーのこの態様の好例の実施形態において、各々の電話2010は、ステグラフィックエンコーダ2036を追加して含む。同様に、各々のセルサイトは、ステグラフィックデコーダ2038を含む。前記エンコーダは、動作し、補助データ信号を電話加入者の音声を表す信号の中に隠す。前記デコーダは、逆の機能を行い、補助データ信号を符号化された音声信号から区別する。この補助信号は、セルの合法性を確認するために動く。

【0412】

好例のステグラフィックエンコーダ2036を図39に示す。

【0413】

示したエンコーダ2036は、ディジタル化音声データ、補助データ、および展望ランダムノイズ(PRN)データにおいて動作する。ディジタル化音声データをポート2040に用い、例えば、A/Dコンバータ2018から与える。ディジタル化音声データは、

8ビット部本を具えてもよい。補助データをポート2042に用い、補助データは、本テクノロジーの1つの形態において、電話2010を固有に識別するバイナリデータのストリームを具えてもよい。（補助データは、通話開始時にセルサイトと自動的に交換される種類の管理上のデータを追加で含んでもよい。）疑似ランダムデータ信号をポート2044において用い、例えば、値“-1”および“1”間でランダムに起こる信号とすることができる。（ますますセルラ電話は、伝播されたスペクトルを受けられる回路網を取り入れており、この疑似ランダムノイズ信号および、このテクノロジーの他の導体は、しはしは、セルラユニットの基本的動作に既に用いられている回路網を“背負う”または共有することができる）。

【0414】

説明に便利のため、エンコード2036に印加される3つのデータ信号すべてを共通のレートでクロック動作させるが、これは実際には必要ない。

【0415】

動作において、補助データおよびPRNデータストリームを論理回路2046の2つの入力部に印加する。回路2046の出力信号は、以下の表に従って、-1および+1の間で切り替わる。

【0416】

【表1】

補助	PRN	出力
0	-1	1
0	1	-1
1	-1	-1
1	1	1

【0417】

（補助データ信号を0および1の代わりに-1および1間の切り替わりとして考える場合、回路2046が1ビット倍率器として動作することが分かる）。

【0418】

したがって、ゲート2046からの出力信号は、随時の値が補助データおよびPRNデータの対応する値に従ってランダムに変化するバイポーラデータストリームである。しかしながら、その中に符号化された補助データを有する、対応するPRNデータを知っている場合、補助データを抽出することができる。

【0419】

ゲート2046からのノイズ様信号を、スケール回路2048の入力部に印加する。このスケール回路は、この入力信号を、サイン初期回路2050によって設定された係数によってスケール化（例えば、倍加）する。示した実施形態において、この係数は、0ないし15間で変動しうる。したがって、スケール回路2048からの出力信号を、補助およびPRNデータと、スケール係数とに従って、各々のクロック周期で変化する5ビットデ

ータワード(4ビットに加え符号ビット)として表すことができる。このスケール回路からの出力信号を、“スケール化ノイズデータ”として考えることができる(しかし、再び、PRNデータを与えた場合、そこから補助データを取り戻すことができる“ノイズ”である)。

【0430】

このスケール化ノイズデータを、加算部2051によってデジタル化音声信号に加算し、符号化出力信号(例えば、標本ごとに2値的に加算された)を発生する。この出力信号は、デジタル化音声データおよび補助データの双方を表す複合信号である。

【0431】

ゲイン制御回路2050は、デジタル化音声データへのその加算が、アナログ形態に変換され、電話加入者によって聞かれた場合、音声データを顕著に変化させないように、加算されるスケール化ノイズデータの振幅を制御する。このゲイン制御回路は、種々の方法において動作することができる。

【0432】

1つは、対数的スケール化機能である。したがって、例えば、10進法値0、1または2を有する音声データ標本を、1または0のスケール係数に対応させてもよく、200以上の値を有する音声データ標本が、15のスケール係数に対応してもよい。一般的に言って、スケール係数および音声データ値は、平方根関係によって対応する。すなわち、音声データの値における4倍の増加は、これらに関係するスケール化係数の値における2倍の増加に対応する。他のスケール化係数は、音声信号の平均パワーから得られるため、線形である。

【0433】

(スケール化係数としてのゼロに対する補足的な参照は、例えば、デジタル化音声信号標本に、本質的に情報内容が無い場合を言及する)。

【0434】

瞬時のスケール化係数が1つの音声信号データ標本を基礎とするよりも満足てことは、スケール化係数がいくつかの標本の方学を基礎とすることである。すなわち、急速に変化しているデジタル化音声データのストリームは、ゆっくりと変化しているデジタル化音声データのストリームよりも、比較的、補助データを隠す恐れがある。したがって、ゲイン制御回路2050を、スケール化係数の設定において、音声データの1次、または好適には2次またはより高次の乗数に應じさせることができる。

【0435】

依然として他の実施形態において、ゲイン制御ブロック2050およびスケール2048を、完全に省略してもよい。

【0436】

(当業者は、前記システムにおける“レールエラー”の可能性を認識するであろう。例えば、デジタル化音声データが8ビット標本から成り、これらの標本が0から255(10進法)までの全体の範囲に及ぶ場合、入力信号へのスケール化ノイズの加算、または入力信号からのスケール化ノイズの減算は、8ビットによって表すことができない出力信号(例えば、-2または257)を発生するかもしれない。この状況を修正する多数のよく理解された技術が存在し、これらのいくつかは順行的であり、これらのいくつかは反動的である。これらの既知の技術に共通して、デジタル化音声データが0-4または241-255における値を持たず、それによって、スケール化ノイズ信号との結合を安全に許可することを指定し、そうしなければレールエラーを生じるデジタル化音声標本を検出し、適応的に修正する対象を含んでいる)。

【0437】

電話2010に戻って、エンコーダ2036は、上記で詳述したようなエンコーダ2036を、A/Dコンバータ2018とデータフォーマッタ2020との間に挿入し、それによって、補助データを作り出すすべての音声送信をステータグラフィックに符号化させる。さらに、電話の動作を制御する回路網またはソフトウェアを、補助データが繰り返す符

号化されるように配置する。すなわち、補助データの全てのビットが符号化された場合、ポイントが端になって戻り、エンコード2036に印加すべき補助データを新たなする。(補助データを、参照を簡単にするためにRAMメモリにおける既知のアドレスにおいて格納してもよい)。

【0428】

示した実施形態における補助データは、音声データのレートの8分の1のレートにおいて送信されることを認識されるであろう。すなわち、音声データの8ビット根本ごとに、補助データの1つの信号ビットに対応するスケール化ノイズデータが送られる。したがって、音声根本が4800根本/秒のレートにおいて送られる場合、補助データを4800ビット/秒のレートにおいて送ることができる。補助データを8ビット記号で構成した場合、補助データを600記号/秒のレートにおいて伝送することができる。補助データが均一な60記号のストリムから成る場合、各符号の音声は、補助データを10回伝送する。(極めてより高い補助データレートを、制限された記号コード(例えば、5または6ビットコード)、ハフマン符号化、等のような、より効率的な符号化技術の力を借りることによって達成することができる。)この補助データの高度に冗長的な送信は、使用すべきスケール化ノイズデータのより小さい歪みを可能にし、依然として、無線送信に関する比較的小さいノイズの多い環境においても確実な復号化を保证するのに十分な信号対ノイズヘッドルームを与える。

【0429】

ここで図40に戻ると、各々のセルサイト2012は、ステータスグラフィックデコード2038を見え、これによって、電話2010によって放送された複合データ信号を分析し、そこから補助データおよびデジタル化音声データを識別し、分離することができる。(このデコードは、好適には、フォーマット化されていないデータ(すなわち、パケットオーバーヘッド、制御および管理上のビットを除去されたデータ、これを説明を簡単にするために図示しない)において動作する。

【0430】

未知の音声信号からの未知の埋め込まれた信号(すなわち、埋め込まれた補助信号)の復号化は、複合データ信号の統計的分析のある形態によって、最適に行われる。上述したこの技術を、ここでも等しく用いることができる。例えば、エントロピーを基礎とするアプローチを利用することができる。この場合において、補助データを(8ビット毎の代わり)に480ビット毎に繰り返す。上記のように、エントロピーを基礎とする復号化プロセスは、複合信号の480番目毎の根本を同様に取り扱う。特に、このプロセスは、複合データ信号の、1番目、481番目、961番目、等の根本を符号化すると共に、PRNデータに加重することから始まる。(すなわち、異なるPRNデータの組、すなわちオリジナルのPRNの組を、すべての、しかし480番目毎のゼロにした基準に加重する。)次に、これらの点の周間の結果として生じる信号(すなわち、480番目毎の根本を変更された複合データ信号)を計算する。

【0431】

次に上記ステップを繰り返し、この時、1番目、481番目、961番目、等の複合データ根本から、これらに対応するPRNデータを減算する。

【0432】

これらの2つの演算の一方は、符号化プロセスを反対に作用(例えば、取り直す)し、結果として生じる信号のエントロピーを減少させ、他方は増加させる。異なるPRNデータを複合データに加重することがそのエントロピーを減少させる場合、このデータは、オリジナルの音声信号からより以前に減算されているに違いがない。これは、補助データ信号の対応するビットが、これらの根本が符号化された場合、“0”になることを示す。(論理図46の補助データ入力における“0”は、その出力基準として、対応するPRN基準の反転したものを発生させ、結果として、対応するPRN基準の音声信号からの減算が生じる)。

【0433】

相違して、複合データから離れたP R Nデータの離れた組の加算、または、(b)複合データからのP R Nデータの離れた組の減算によって、より低くなった場合に注意することによって、補助データの最初のビットが(a)“0”であるか、または(b)“1”であるかを決定することができる。(先路の用途において、種々の歪み現象の存在において、複合信号を十分に劣化させ、離れたP R Nデータの加算も減算も、実際にエントロピを減少させないようにしてもよい。代わりに、双方の演算は、エントロピを増加させるであろう。この場合において、“適切な”演算を、どの演算がエントロピを少なく増加させるかを観察することによって、識別することができる)。

[0434]

エントロピが、(a)複合データへのP R Nデータの離れた組の加算、または、(b)複合データからのP R Nデータの離れた組の減算によって、より低くなった場合に注意することによって、補助データの最初のビットが(a)“0”であるか、または(b)“1”であるかを決定することができる。(先路の用途において、種々の歪み現象の存在において、複合信号を十分に劣化させ、離れたP R Nデータの加算も減算も、実際にエントロピを減少させないようにしてもよい。代わりに、双方の演算は、エントロピを増加させるであろう。この場合において、“適切な”演算を、どの演算がエントロピを少なく増加させるかを観察することによって、識別することができる)。

[0435]

次に、上記演算を、2番の根本から始めた複合信号の間隔をおいた根本(すなわち、2、4、8、2、9、6、2、...)のグループに行く。結果として生じる信号のエントロピは、補助データ信号の第2ビットが“0”または“1”のいずれであるかを示す。コードワードのすべての480ビットが識別されるまで、複合信号における間隔を置いた根本の478のグループを同様に続ける。

[0436]

上述したように、複合データ信号とP R Nデータとの相互関係を、統計的検出技術として使用することができる。このような演算は、現在の文脈において、その符号化表現が、先天的に、少なくとも大きい部分において、調査され、知られている補助データから、容易になる。(本テクノロジーの1つの形態において、補助データは、セルラシステムは既に受信し、認識している、通信開始時に交換される認証データを基礎としており、他の形態(以下に詳述する)において、補助データは、予め決められたメッセージを見る。)したがって、前記問題を軽減することができ、(未知の信号全体を捜すよりも)期待される信号が存在するかどうかを決定することができる。さらに、データフォーマット2020は、複合データを既知の長さのフレームに分解する。(既知のG S M実現化において、音声データを、各々114データビットを伝送するタイムスロットにおいて送る。)補助データを必要に応じて拡張することによって、補助データの各々の繰り返しを、例えば、このようなデータのフレームの開始において開始させることができる。これは、114の可能なビットアライメント毎の113を無視することができるため、相関関係決定を非常に簡単にする(先天的に既知の補助データが無いとしても、復号化を助ける)。

[0437]

再び、この無検数検出は、ノイズ中の既知の信号を検出することの現在ありふれた問題を提出し、前に考察したアプローチをここで等しく用いることができる。

[0438]

補助信号の場所が先天的に既知である(またはより正確に、上述したように、いくつかの別個の場所のうちの1つになることが既知である)場合、前記整合フィルタアプローチを、しばしば、離れたP R Nデータの組と、これらに対応する複合信号の平均値を用いた引当との簡単なベクトルドット積に減少させることができる。(P R Nデータを離れたにする必要はなく、以前に言及した英国特許公開明細書第2196167号におけるような、接近するバーストに達してもよいことに注意されたい。ここで、メッセージにおける特定のビットは、それに関連する接近したP R N値を有する。)このようなプロセスは、P R Nデータが正の場合、補助データ信号の対応するビットは“1”であり、ドット積が負の場合、補助データ信号の対応するビットは“0”である。構成した複合信号内の補助データ信号のいくつかのアライメントが可能である場合、この手順を各々の候補アライメントにおいて繰り返し、最高相関関係を生じるものを真として選択する。(一度、正しいアライ

メントが補助データ信号の1つのビットに対して決定されると、他のすべてのビットのアラインメントを、そこから決定することができる。ひょっとすると“同期化”としてより知られている“アラインメント”を、主として、音声信号それ自体をロックオンして追跡し、セルユニットの基本的な機能を考慮する全く同じ機構によって達成することができる。

【0439】

セキュリティの考え

今説明した実施形態のセキュリティは、大きな部分において、PRNデータのセキュリティおよび/または補助データのセキュリティに依存する。以下の考察において、これらのデータのセキュリティを保証する多くの技術のいくつかを考察する。

【0440】

第1の実施形態において、各々の電話2010は、その電話に固有の長いノイズキーを与える。このキーを、例えば、ROMに格納された高度に固有の10000ビットストリングとしてもよい。(大部分の用途において、キーは、使用してもよいこれよりも実務的に短い)。

【0441】

中央局2014は、すべての許可された電話に関するこのようなキーデータを格納する保障ディスク2052へのアクセスを有する。(このディスクを、中央局それ自体から離してもよい)。

【0442】

電話を使用する度に、このノイズキーからの50ビットを識別し、決定論的擬乱ランダム数発生器に対する種として使用する。このPRN発生器によって発生されたデータは、その通話に関するPRNデータとして働く。

【0443】

この50ビット種を、例えば、通話のために電話を使用する度に0ないし9950のオフセットアドレスを発生する、電話におけるランダム数発生器によって決定することができる。このオフセットアドレスにおいて開始するノイズキーの55ビットを、前記種として使用する。

【0444】

通話開始中、このオフセットアドレスを、電話によって、セルサイト2012を経て中央局2014に送信する。ここで、中央局におけるコンピュータは、オフセットアドレスを使用し、その電話に関するノイズキーのその複製をインデックス化する。それによって、中央局は、電話において識別されるのと同じ50ビット種を識別する。次に、中央局2014は、これらの50ビットをセルサイト2012に中継し、ここで、電話におけるものと類似した決定論的ノイズ発生器が、この50ビットキーに対応するPRNシーケンスを発生し、その複出器2038に供給する。

【0445】

前述のプロセスによって、PRNの同じシーケンスが、電話およびセルサイトの双方において発生する。したがって、電話によって音声データにおいて符号化された補助信号を、セルサイトに安全に送信することができ、セルサイトによって正確に復号化することができる。この補助データが期待される補助データ(例えば、通話開始時に送信されたデータ)と一致しない場合、この通話を不正としてフラグを立て、適切な矯正動作を起こす。

【0446】

通話開始情報の無線送信を盗み聞いている人は、電話によってセルサイトに送信されるランダムに発生されたオフセットアドレスのみを傍受できることが、認識されるであろう。このデータは、単独では、通話を盗むことにおいて役に立たない。ハッカーが、中央局からセルサイトに与えられた信号にアクセスしたとしても、このデータも本質的に役に立たず、与えられるすべての50ビット種である。この種は、近い各々の通話に関して異なる(9950の通話ごとに1つのみ繰り返し)ことから、ハッカーには無益である。

【0447】

関係するシステムにおいて、10000ビットノイズキーの全体を、種として使用することができ、通話開始中に電話によってランダムに発生されたオフセットアドレスを使用し、その種から結果として得られるPRNデータにおいて、そのセッションに使用するべきPRNデータを開始することを示す。(1秒あたり4800音声フレームとして、4800PRNデータが1秒あたり必要であり、すなわち17万程度のPRNデータが1時間あたり必要である。したがって、この変形実施形態におけるオフセットアドレスは、上述したオフセットアドレスよりもはるかに大きくなると思われる)。

【0448】

この変形実施形態において、復号化に使用されるPRNデータを、好適には、中央局において10000ビット種から発生し、セルサイトに中継する。(セキュリティ上の理由のため、10000ビットノイズキーは、中央局のセキュリティを離れるべきではない)。

【0449】

上記システムの変形において、この逆にするよりも、オフセットアドレスを、中央局によって、またはセルサイトにおいて発生し、通話開始中に電話に中継することができる。

【0450】

他の実施形態において、電話1020に、中央局における保障ディスク2052において格納された種のリストと一致する、1回種のリストを与えてもよい。新たな通話を始めるために電話を使用する度に、このリストにおける次の種を使用する。この配置によって、種に関する交換にデータは必要なく、電話およびキャリアの各々は、独立に、どの種を使用し、現在のセッションのための疑似ランダムデータシーケンスを発生するかを知る。

【0451】

このような実施形態において、キャリアは、電話がその種のリストをほぼ使い果たす時を決定することができ、代わりのリストを(例えば、電話に対して即時に与えられる管理データの一部分として)送信することができる。セキュリティを増すために、キャリアは、電話を手動再プログラミングに戻し、この変動しやうい情報の無線送信を回避することを要求してもよい。代わりに、代わりの種リストを、種々の既知の技術のいずれかを使用して、無線送信のために暗号化することができる。

【0452】

実施形態の第2のクラスにおいて、セキュリティは、PRNデータのセキュリティからだけでなく、そこから符号化された補助メッセージデータのセキュリティからも派生する。あるこのようなシステムは、256の可能なメッセージからランダムに選択された1つの送信に頼っている。

【0453】

この実施形態において、電話におけるROMは、256の異なるメッセージを格納する(各々のメッセージを、例えば、長さにおいて128ビットとしてもよい)。通話を開始するために電話を操作した場合、電話は、1ないし256の番号をランダムに発生し、この番号は、これらの格納されたメッセージに対するインデックスとして働く。このインデックスを、通話開始中にセルサイトに送信し、中央局に、同じ256のメッセージを含む保障ディスクにおける一致データベースからの期待されるメッセージを識別させる。(各々の電話は、メッセージの異なる集合を有する。)(代わりに、キャリアは、通話開始中にインデックス番号をランダムに選択し、それを電話に送信し、そのセッション中に使用するべきメッセージを識別してもよい。)保障システムに企てられる攻撃が現実的に数学的のみである理論的に純粋な世界において、これらの付加的なセキュリティのレイヤの多くは、過剰に見えるかもしれない。(メッセージ自体を異ならせるような、これらのセキュリティの付加レイヤの追加は、単に、実際の公衆に機能する保障システムの設計者が、このテクノロジの中心的管理の数学的セキュリティを危うくするかもしれない、ある実用化経路に直面するであろうことを認める)。

【0454】

その後、その通話中に電話によって送信されたすべての音声データを、インデックス化

メッセージと共にステガノグラフィ的に符号化する。セルサイトは、期待されるメッセージの存在に関して、電話から受けたデータを検査する。そのメッセージが正しい場合、または、異なるメッセージが代わりに復号化された場合、その通話を、不正であるとしてフラグを立て、矯正動作を起こす。

【0455】

この第2の実施形態において、符号化および復号化に使用されるPRNデータを、望むだけ簡単に複製にもすることができる。簡単なシステムは、各々のセルに対して、同じPRNデータを使用する。このようなデータを、例えば、電話に対して固有であり、中央局によっても知られている固定されたデータ（例えば、電話識別子）を種とする決定論的PRN発生器によって発生してもよく、または、万能ノイズシーケンスを使用することができる（すなわち、同じノイズシーケンスを、すべての電話に対して使用することができる）。または、疑似ランダムデータを、（例えば、例えば目的電話番号、等を識別する。通話開始中に送信されるデータを基礎とする）通話毎に変化するデータを種とする決定論的PRN発生器によって発生することができる。いくつかの実施形態は、疑似ランダム数発生器に、前の通話からのデータの種を内いてもよい（このデータは、電話およびキャリアに対して必然的に既知であるが、盗人には未知であると思われるため）。

【0456】

もちろん、前記2つのアプローチからの要素を、種々の方法において結合することができる。他の特徴を付加することができる。前記実施形態は、単に好例であり、使用することができる無数のアプローチのカテゴリを作りはじめはしない。一般的に言って、電話およびセルサイト/中央局の双方によって必然的に知られるまたは知られるようなデータも、補助メッセージデータ、またはそれを符号化するPRNデータのいずれかに対する基礎として使用することができる。

【0457】

本テクノロジーのこの態様の好適実施例は、電話加入者のデジタル化音声の持続時間の間中、補助データを各々ランダムに符号化するため、補助データを、受信されたオーディオのどのような短い根本からも復号化することができる。本テクノロジーのこの態様の好適な形態において、キャリアは、ステガノグラフィ的に符号化された補助データを、（例えば、10秒ごと、またはランダムな間隔において）繰り返し検査し、期待される属性を持ちつづけていることを保証する。

【0458】

前記考察は、セル電話からの送信をステガノグラフィ的に符号化することに焦点を置いていたが、同様に、セル電話への送信をステガノグラフィ的に符号化できることが認識されるであろう。このような配置は、例えば、管理データ（すなわち、非音声データ）のキャリアや個人への電話への配送において適切である。この管理データを、例えば、目標とされるセル電話（またはすべてのセル電話）を中央局から再プログラムする、（上述したオンタイムバンドシステムを用いるシステムに関する）繰り返しを更新する、良く知らない局所領域に属するデータを“徘徊する”セル電話に知らせる、等を使用することができる。

【0459】

いくつかの実施形態において、キャリアは、セル電話に、そのセル電話がそのセッションの残りの間にキャリアへの送信において使用する種をステガノグラフィ的に送信してもよい。

【0460】

前記考察は、ベースバンドデジタル化音声データのステガノグラフィ的符号化に焦点を置いていたが、当業者は、中間周波数信号（アナログまたはデジタル）を、同様に、本テクノロジーの原理に従ってステガノグラフィ的に符号化できることを認識するであろう。ポストベースバンド信号の種が、これらの中間周波数信号のバンド幅がベースバンド信号と比べて比較的に広く、より多くの補助信号をその中に符号化することができる、または、一定の量の補助信号を送信中により頻りに繰り返すことができることである。（中間

信号のステガノグラフィ的符号化を用いた場合、符号化によって導入される変動が、パケットフォーマットによって支持されるエラー訂正設備を考慮して、管理データの確実な送信に影響するほど大きくならないように注意すべきである。

【0461】

当業者は、補助データそれ自体を、既知の方法において配置し、デコーダ8によるエラー検出、またはエラー検出能力を援助させることができることを認識するであろう。興味を持った読み手は、このような技術を検討する多くの容易に利用可能な教科書のうちの1つ、例えば、ローバウ、エラー符号化クックブック、マクロール、1996を参照されたい。

【0462】

本テクノロジーのこの態様の好適実施形態を、パケット化データを使用するセルラシステムの変態において説明したが、他の無線システムは、このような便利に構成されたデータを用いない。構成化を同期化の援助として使用できないシステムにおいて、同期化を、本人の先行出願に詳述するような技術を使用して、複合データ信号内で達成することができる。あるクラスのこのような技術において、補助データそれ自体が、その同期化を容易にする特徴を有する。他のクラスの技術において、補助データは、アライメントおよび検出を容易にするように設計された1つ以上の埋め込まれたキャリアパターンを変調する。

【0463】

以前示したように、本テクノロジーの原理は、上記で詳述したステガノグラフィ的符号化の特別な形態との使用に限定されない。実際は、既知の、または後に発明されるどのようなステガノグラフィ的符号化技術も、上記で詳述した方法において、セルラ（または、他の無線、例えば、PCS）通信システムのセキュリティまたは機能を増すために使用することができる。同様に、これらの原理は、無線電話に限定されず、どのような無線通信にも、この形式の“バンド内”チャネルを与えることである。

【0464】

本人のテクノロジーを実現するシステムは、専用のハードウェア回路素子を見えることができるが、より一般的に、関係するRAMおよびROMメモリを有する適切にプログラムされたマイクロプロセッサ（例えば、電話2010、セルサイト2012、および中央局2014の各々におけるこのようなシステム）を見えることもできることを認識されるであろう。

【0465】

ビットセルによる符号化

前記考察は、個々の画素の値の増加または減少に焦点を置き、擬似ランダム信号に結合された補助データ信号の符号化を反映する。以下の考察は、補助データを、擬似ランダム化無しで、ここでビットセルと呼ぶ、画素のパターン化されたグループによって符号化する変形実施形態を詳述する。

【0466】

図41Aおよび41Bを参照して、2つの説明的な2×2ビットセルを示す。図41Aを使用して補助データの“0”ビットを表し、図41Bを使用して“1”ビットを表す。動作において、下にある画素の画素を、ビットセルのノッチ値に従って引き上げまたは引き下ろし、これらの2つのビット値の1つを表す。（以下に詳述するように、画素の所定の画素または領域を引く大きさを、多くの因子の関数とすることが可能である。特徴パターンを規定することが、引く含意である。）復号化において、符号化画素の相対的バイアスを（上述した技術を使用して）調査し、符号化画素の各々の対応する領域に関して、2つのパターンのどちらを表すかを識別する。

【0467】

この実施形態において、補助データを明白にランダム化しないが、ビットセルパターンを、上述したように、“設計された”キャリア信号とみなしてもよいことが認識されるであろう。

【0460】

この「設計された」情報キャリアの、前記実施形態の擬似ランダムノイズとの交換は、ビットセルバターン化が、フォーエ空間におけるそれ自体を明らかにするという利点をもたらす。したがって、ビットセルバターン化は、上述したサブリミナルデジタルグラフィックのように曲くすることができ、展覧し画像の登録を助け、スケール/回転エラーを除去する。ビットセルのサイズと、それにおけるバターンとを変化させることによって、空間変換距離におけるそれによって与えられるエネルギーの場所を変更することができ、代表的な画像エネルギーからのインピーダンスを最適化し、検出を容易にする。

【0461】

（前記考察は、補助データで、PRN信号によるランダム化無しで、直接符号化することと考えたが、他の実施形態にいて、もちろん、ランダム化を使用することができる。）。

【0470】

概念的により適合した署名

既に説明した実施形態のうちのいくつかにおいて、署名エネルギーの大きさを領域間に基つて適合させて、画像中で目に見えなく（又は、音声中で聞こえにくく）する。以下の説明中、出願人は、画像中の隠蔽署名エネルギーの問題、これにより課された分離の問題、及びこれら問題の各々の解決を、更に特別に考察する。署名プロセスの目的は、単なる動作を超えて、所定のユーザ/クリエイターによる固定された「見えやすさ/許容しうるしきい値」のある形態に適合しながら嵌め込まれた署名の「数字の検出可能性」を最大にすることである。

【0471】

この目的に対して設計するためのサービスに当たり、以下の3軸パラメクススペースを考え、この場合、これら軸のうちの二つを半軸（正のみ）とし、第3の軸を、全軸（正負）とする。軸のこのセットは、ユークリッド3次元の通常の8個のスペースのうち二つを規定する。事象を洗練するとともに「分離する価値がある」パラメータが（拡張された局所的な見えやすさのマトリックス）のようなシーン上に現れると、それらは、（一般的には）それら自体の半軸を規定するとともに3次元を超える以下の例に拡張することができ。

【0472】

署名設計目的は、上記スペースの座標に基づく局所的なパンパに「サイン」を最適に割り当て始め、その間、基本的には、実際の用途において動作を迅速にする必要があることを留意しておく。先ず、3軸を以下のようにする。二つの半軸をx及びyとし、全軸をzとする。

【0473】

x軸は、単一パンパの輝度を表す。基本的な概念は、僅かなエネルギーを搾りだして、ぼやかし置かれた領域に対して領域を明るくすることである。重要なことは、真の「サイココーニニア」装置領域「輝度値（直素DN）」が現れると、輝度値が他の作動値（例えば、 $C^* \times y$ ）に結合する場合には、この軸は不必要となる。この際、これは、ここで現在の類似線形輝度符号化の顕微鏡的な最適化が原因となっている。

【0474】

y軸は、パンパそれ自体が見つける範囲内の隣接する「局所的な隠蔽ポテンシャル」である。基本的な概念は、眼が平坦領域のような微妙な変化を検出することができるので、平坦領域が低隠蔽ポテンシャルを有することである。非常にスムーズな長いラインの「縦横及び切断」も度分目に見えるので、長いライン及び長いエッジは、隠蔽ポテンシャルが高くなる傾向にある。長い及び短いこれらの概念は、処理時間の問題及びパラメータのような慎重な定量化に必要な処理手段の問題に直接結びつく。y軸の動作モデルの展開は、必然的に一部の複雑しい芸術家の経験論に対して一部の理論を伴う。y軸部分寄せ集めるに従ってより知識が増えるので、それらは分裂して、価値がある場合にはそれら自体の独立した軸となる。

【0475】

と軸は、(後に説明するように)「ゲインを伴う又はゲインに反する」軸であり、他の二つが半軸であるのに対してこれは全軸である。基本的な概念は、所定の入力ハンプが、その位置で「1」又は「0」に符号化した入力に対して平均存在するバイアスを有し、それはある程度、用いられる読出しアルゴリズムの関数となり、その(バイアスの)大きさは、 y 軸の「隠蔽ポテンシャル」に幾分相関し、それを、当該ハンプにどの程度の大きさのトワーク値を割り当てるかを決定する際に変換として、好適に用いることができる。相対する基本概念は、ハンプが既に友達である(すなわち、その近隣に対するバイアスが所望のΔ値となる傾向にある)場合、それを大幅に変えてはいけなく、その既に自然な状態は、局所的な価値値を大幅に、場合によっては全く変えることなく、復号化に必要なデータエネルギーを提供する。それに対して、ハンプが最初に敵である(すなわち、その近隣に対するバイアスが、符号化によって課されるべきと考えられるΔ値から離れる傾向にある)場合、それを大幅に変えなさい。この後者の動作は、ポイントが目に見えにくくなる傾向がある(非常に局所的なぼんやりした動作)その近隣に対するこのポイントの偏位を減少させるとともに、復号化の際に検出可能な追加のエネルギーを供給する。これら二つの場合、ここでは、これら二つの場合を、「ゲインを伴う」及び「ゲインに反する」と称する。

【0476】

既に説明したような問題の一般的な概念は、数年間十分である必要が。明らかに、クロミナンスの問題を加えることは、規定をやや拡張し、より大きな見えやすさに対する署名バンプとなり、圧縮の問題に適用される人間の見えやすさの調査を、正反対の理由がない場合にはこの区域に等しく適用することができる。ここでは、典型的な用途で用いることができる原理を説明する。

【0477】

スピードのために、局所的な隠蔽ポテンシャルを、直素の 3×3 隣接に基づいてのみ計算することができる。スピードの問題以外には、より大きいものを支持するデータ又は固有の理論も存在しない。設計の問題を要約すると、 y 軸の見えやすさ、輝度をこれに結合する方法、及び些細な友達/敵の非対称である。ガイド原理は、平坦区域を単に零とし、従来の純粋な最大又は最小領域を「1、0」すなわち最大値とし、「局所的なライン」、「円滑な傾斜」、「鋭型ポイント」を有するとともにこれらの間のどこかで何も拒絶しないことである。

【0478】

典型的な用途は、6個の基本パラメータ、1)輝度、2)局所的な平均の差、3)「ゲインに伴う又はゲインに反する」非対称因子、4)最小線形因子(平坦対ライン対最大の粗い読み)、5)ヒット平面バイアス因子、6)全体ゲイン(ユーザの単一トップレベルゲインノブ)を用いる。

【0479】

輝度パラメータと、局所的な平均からの差のパラメータは、線形的であり、その使用は、本明細書以外で指定される。

【0480】

非対称因子は、2より上の差軸の「ゲインに反する」側に適用される単一スカラーである。

【0481】

最小線形因子は、明らかに粗い読み、それを 3×3 隣接セッティングでさえあるサービスを行うべきである。この概念は、真の2D最小及び最大が 3×3 隣接の中央画素を横断する4ラインの各々に沿って非常にきままわされ、縦向の4ライン又はエッジが四つの線形プロフィールと少なくとも一つをのぼす傾向にある。四つの線形プロフィールをそれぞれ長き方向に3画素とする。すなわち、右上画素-中央-右下、真上-中央-真下、右左-中央-左下、右側-中央-左側)行方向の三つの画素に適用されるようなエントロピーのマトリックスを選択し、四つの全ての線形プロフィール上でこれを実行し、その後、「 y 軸」

として用いるべき最大パラメータに対して最小値を選択する。

【0482】

ビット平面バイアス因子は、2画、すなわち以前に空の面及び次に空の面を有する面白いものである。前者の場合、単に、署名されていない画像を「読み出す」とともに全てのバイアスが全てのビット平面に対して外れる場所を見て、全体的に所望のメッセージに反して進行するビット平面の「全体ゲイン」を簡単に引き上げるとともに、他のもののみ、すなわちそのゲインより僅かに低いものを取り除く。後に空の場合、以前に空のビットプレーンバイアス及びここでリセットした他のパラメータを有する全署名プロセスを実行し、例えば、画像をプリントした後に定着するラミネーションの大きなJPEGB圧縮ANDモデルの「タスクルト歪み」を介した署名画像を実行し、その画像を読み出すとともに、どのビットプレーンが混在している又はエラー状態にあるかを発見し、ビットプレーンバイアスを適切に補償し、アタラクチックを実行する。拡散プロセスを行う良好なデータを有する場合、このステップを1回実行するだけでよく、すなわち、ハンチックタイス(Van-Clitterize)プロセスを容易に行うことができる(トウィークに適用したある経路係数でプロセスを繰り返すために曖昧に参照する)。

【0483】

最後に、全体ゲインが存在する。その目的は、この単一変数を、所望の場合には少しでも興味のあるユーザが調整することができるトップレベル「強度ノブ」(より典型的には、「固面的なユーザインタフェースのスライダースは他の制御)にすることである。非常に興味があるユーザは、進化したメニューを下げ、他のうちのいくつか上で経験的に処理する。

【0484】

目に見える透かし。

ある用途において、目に見える徽候を画像に供給して、それがステガノグラフィックに符号化されたデータを含むことを表示することが望ましい。一例において、この徽候を、画像の1コーナーに付与される僅かに目に見えるロゴ(時々「透かし」と称される。)とすることができ、これは、画像が「スマートな」画像であり、微に加えてデータを搬送することを示す。電報は、一つの適切なロゴである。

【0485】

他の用途

開示した技術に対する一つの用途は、Adobe's Photoshop softwareのような画像処理ソフトウェアを用いるためのマーケティング/デコーディング「アラタイン」のようのものである。一旦、このような画像のマーケティングが広かると、このようなソフトウェアのユーザは、はめ込まれたデータを画像から復号化するとともに、公衆登録簿を調べ、画像の所有者を識別する。ある例では、保護は、適切なロイヤリティの支払いがユーザの画像の使用に対する所有者に行われる筈として作用することができる(図示した例において、登録簿は、データベースに結合され、WWWを介してアクセス可能なインターネットのサーバとなる。データベースは、画像それ自体が符号化される情報コードによって示された、カテゴリーを作成した画像の詳細な情報(例えば、所有者の名前、住所、電話番号や、画像に行うことができる種々のタイプの使用に対する料金表)を含む。画像を復号化する者は、このように集めたコードを用いて所有者を質問し、所望の場合には、画像の所有者に著作権のロイヤリティを電子的に支払う)。

【0486】

他の用途は、スマートなビジネスカードであり、この場合、ビジネスカードに、目立たない、機械で読み出し可能なはめ込まれたコンタクトデータを有する写真を設ける(同一機能を、データをはめ込むカードの表面マイクロプロセッサを変化させることによって達成する)。

【0487】

更に別の期待できる用途は、内容規格におけるものである。テレビジョン信号、インターネット上の画像、及び他の内容源(音声、画像、ビデオ等)は、外部的に関連するよりは

内容それ自体に実際にほめ込まれた「適正」（すなわち、セックス、暴力、子供に対する適正等に対する等級）を表すデータを有することができる。テレビジョン受像機、インターネットサーフィンソフトウェア等は、（例えば、全体的なコード後導化の使用による）このような適正の等級を明確に理解することができ、適切な動作（例えば、画像又はビデオを見ることを許可しない、又は音源を再生しない。）を行うことができる。

[0488]

これまで説明したうちの簡単な例において、ほめ込まれたデータは、一つ以上の「フラグ」ビットを有することができる。あるフラグは、「子供に対する不適切」を示す（他のものを、例えば「この画像はコピーライトされています」又は「この画像は公衆領域です」とすることができる。）。このようなフラグビットを、ほめ込まれたメッセージとは別個の制御ビットのフィールド内にある、すなわち、それ自体をメッセージとすることができる。これらのフラグビットの位置を検査することにより、デコーダのソフトウェアは、画像の種々の特性のユーザを迅速に知らせることができる。

[0489]

（制御ビットを、サブミリアルグラフィックに対して既知の画像の既知の位置で符号化することができる、ほめ込まれたデータ（例えば、その長さ、そのタイプ等）のフォーマットを示すことができる。このように、これら制御ビットは、従来のファイルヘッダで時々搬送されるデータに類似しているが、この場合、これらを、ファイルに対して考察する代わりに、画像内にはめ込む）。

[0490]

製品のマーキングの分野は、一般に、普通のバーコード及び全体の製品コードによって十分利用されている。しかしながら、所定の用途において、このようなバーコードは、（例えば、エステティックを考慮する場合、又は、セキュリティに関する場合）不所望である。このような用途において、出願人の技術は、無害のキャリア（例えば、製品に関する写真）を介して、又は製品の表面のマイクロホロジー又はその上のラベルを符号化することにより、製品にマークすることができる。

[0491]

ステファノグラフィに暗号化及び／又はディジタル署名技術を有効に組み合わせる安全性を増大させる一非常に多くて詳細に説明できない一用途がある。

[0492]

医療記録は、証明が重要な分野に現れる。—フィルムに基づく記録又は文書のマイクロホロジーに適用されるステファノグラフィ原理を用いて、不正に対する保護を行うことができる。

[0493]

多くの産業、例えば自動車及び旅客機は、重要な部分をマークする札を信頼する。しかしながら、このような札は容易に取り除かれ、時々偽造される。安全性がより望まれる用途において、会社の部分をステファノグラフィにマークして、目立たない識別／証明札を提供することができる。

[0494]

本明細書で見た種々の用途において、相連するメッセージを、画像の相連する領域によって関連的に搬送することができる（例えば、画像の相連する領域は、相連するインターネットURLを提供することができる、フォトコラージュの相連する領域は相連する写真家を識別することができる。）。他のメディア（例えば、音声）についても同様である。

[0495]

あるソフトウェアビジュアルは、データの境がデータ波形を通る際のデータを観察して、他のデータの境に相互作用させる。このようなときにおいて、このような境が強調であり、正当にそれ自体を識別する必要がある。ここでも、ステファノグラフィの技術により、偽造の信頼性を増すことができる。

[0496]

最後に、メッセージ変換コード—ステファノグラフィックに符号化されたメッセージが

、内在するステファノグラフィックなコードパターンを実際に変える同様のシステムーは、新たなレベルの洗練及び安全を提供する。このようなメッセージ変換コードは、時間変化要素が安全性を高めるのに重要なアラシックキャッシュカードのような用途に非常に好適である。

【0497】

また、使用者が、既に説明したようなステファノグラフィックな符号化の特定の形態を好む場合、本明細書に開示したものは別の用途を、他のステファノグラフィックなマーキング技術を用いて広く実現することができ、その多くは従来既知である。また、同様に、本明細書は、画像に対してこの技術の用途を強調したが、その原理を、一般に、音声、物理的なメディアのこのような情報、又は情報の他の任意のキャリアのほめ込みにも同様に適用することができる。

【0498】

多数の実施の形態及びその変形を参照してこの技術の原理を説明したが、この技術を、この原理を逸脱することなく装置中で実装することができる。したがって、以下の請求の範囲及びその等価物の範囲内で全ての実施の形態を、本発明として請求する。

【図面の簡単な説明】

【0499】

【図1】 2つの軸において分離された1次元デジタル信号の簡単なつ古典的な線図である。

【図2】 “微細”の認証信号を他の信号上に埋め込む処理の、ステップの詳細な記述による全体的な概観である。

【図3】 オリジナルの疑わしいコピーをどのように検証するかについての断片的説明である。

【図4】 本発明の他の実施例による検証情報によってフィルムを前露光する装置の線図である。

【図5】 本発明の“ブラックボックス”実施例の図表である。

【図6】 図5の実施例のブロック図である。

【図7】 異なるコードワードを有する同じノイズデータを有する入力データの連続する組を符号化するのに適合した図6の実施例の変形例を示す。

【図8】 特有のコード番号を有するビデオテープ製造の各々のフレームを符号化するのに適合した図6の実施例の変形例を示す。

【図9】 A〜Cは、本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。

【図10】 標準ノイズコードの検出において使用される集積回路を示す。

【図11】 図10の実施例において使用することができる標準ノイズコードを検出する処理の流れを示す。

【図12】 本発明の他の実施例による複数の検出器を使用する実施例である。

【図13】 疑似ランダムノイズフレームを画像から発生する実施形態を示す。

【図14】 信号の統計を復号化の補助においてどのように使用できるかを示す。

【図15】 どのような署名信号を使用し、予測される歪み（例えば、MPEG）の観点におけるその歪平きを増加かを示す。

【図16】 ファイルについての情報をヘッダおよびファイル自体において評述する実施形態を示す。

【図17】 ファイルについての情報をヘッダおよびファイル自体において評述する実施形態を示す。

【図18】 回転対象パターンを使用する実施形態に関する詳細を示す。

【図19】 回転対象パターンを使用する実施形態に関する詳細を示す。

【図20】 回転対象パターンを使用する実施形態に関する詳細を示す。

【図21】 曲線よりも“ハンダ”の符号化を示す。

【図22】 セキュリティカードの模様を詳細に示す。

- 【図23】セキュリティカードの態様を詳細に示す。
【図24】セキュリティカードの態様を詳細に示す。
【図25】セキュリティカードの態様を詳細に示す。
【図26】セキュリティカードの態様を詳細に示す。
【図27】固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク方法を説明する図である。
【図27A】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。
【図27B】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。
【図28】写真識別文庫またはセキュリティカードの図である。
【図29】サブミナルデジタルタテキールを実現することができる2つの実施形態を示す。
【図29A】図29の実施形態における変形例を示す。
【図30】サブミナルデジタルタテキールを実現することができる2つの実施形態を示す。
【図31】A及びBは、2つの傾斜軸に沿った空間周波数の位相を示す。
【図32】A～Cは、第1、第2および第3同心リンクに沿った空間周波数の位相を示す。
【図33】A～Eは、傾斜軸を使用するサブミナルタテキールに対する登録プロセスにおけるステップを示す。
【図34】A～Eは、同心リンクを使用するサブミナルタテキールに対する登録プロセスにおけるステップを示す。
【図35】A～Cは、傾斜軸を使用するサブミナルタテキールに対する他のステップを示す。
【図36】A～Dは、2DFFTを必要としない他の登録プロセスを示す。
【図37】サブミナルタテキールに対する登録プロセスを要約するフローチャートである。
【図38】好例の無線電話システムの主な部品を示すブロック図である。
【図39】図38のシステムの電話において使用することができる好例のステガノグラフィ的エンコードのブロック図である。
【図40】図1のセルサイトにおいて使用することができる好例のステガノグラフィ的データのブロック図である。
【図41】AおよびBは、符号化の一形態において使用する好例のビットセルを示す。

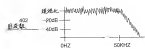
(9 8)

特開2005-51793(P2005-51793A)

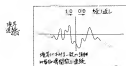
【図9A】



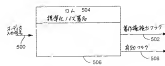
【図9B】



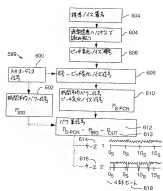
【図9C】



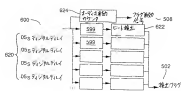
【図10】



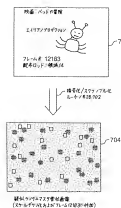
【図11】



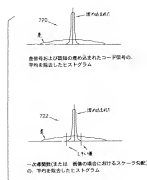
【図12】



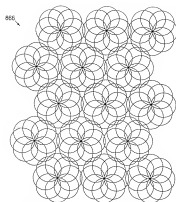
【図13】



【図14】

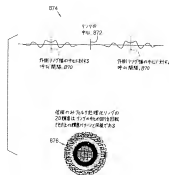


【図19】



オリシチル素を置いた。これと同一空間のモザイクパターンを形成。すべての要素/ノットパターンは、著名のような同じ特徴を輸送することである。または、各々のステップグラフィック意味における新たなメッセージを輸送することである。

【図20】



【図21A】

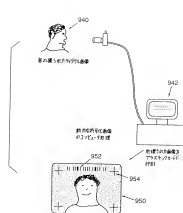


【図21B】

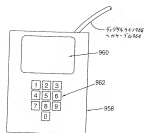
	2	3	4	5	6	7	0
6	7	0	1	2	3	4	
2	3	4	2C	C			
6	7	0	1	2	3	4	

多くの数値的パターンの構造を構築するのに役立つ。これらの構造はビットパターンに組み込まれる。ここで、0-7のインデックスを有するビットパターンに組み込まれる。ビットパターンは、0-7のインデックスを有するビットパターンに組み込まれる。

【图22】



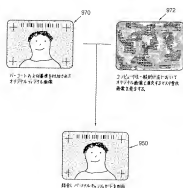
【图23】



基本的な光学スキャナ、メモリバッファ、通信装置およびマイクは、プロセッサを含む。

客は単に、プラスチックカードを窓に置き、パーソナル識別番号(付加したセキュリティのために置く)か、そうでないかを予め任意に決めることができる。換取り引きは、数秒以内に承認または否認される。

【例24】

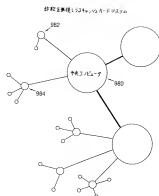


代議的な商取引引きステップ

- [illegible]

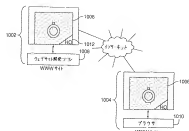
【图25】

【図26】

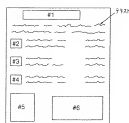


キャッシュカードシステムの基盤は、無線LANカードシステム550と構成する。図26は、無線LANカードシステム550の構成を示す。サーバ/ルータは、無線LANカードシステム550と接続されている。サーバ/ルータは、無線LANカードシステム550と接続されている。サーバ/ルータは、無線LANカードシステム550と接続されている。

【図27】



【図27A】



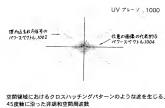
【図27B】



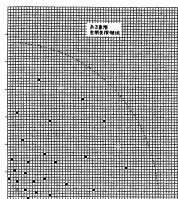
【図28】



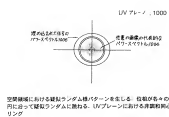
【図29】



【図29a】



【図30】



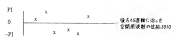
(1 0 5)

特開2005-51793(P2005-51793A)

【図31A】



【図31B】



【図32A】



【図32B】



【図32C】



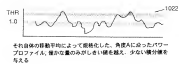
【図33A】



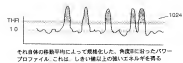
【図33B】



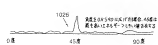
【図33C】



【図30】



【図31】



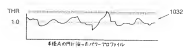
【図32】



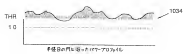
【図33】



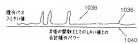
【図34C】



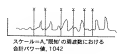
【図34D】



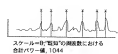
【図34E】



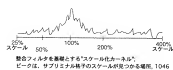
【図35A】



【図5B】



【図5C】



【図5A】



サブリミナルグタキニール
が配置されてくるかもしれない
位置のオシロスコプス。

【図5B】

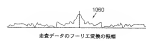


「オシロ」も、画面の中心を通過して
所定の位置に当たっている。

【図36C】



【図36D】

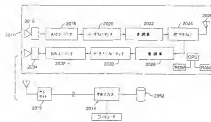


【図37】

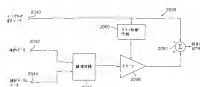
プロセスステップ

1. 用意にある要素
2. 2D FFT
3. 2Dフーリエ変換の発生、例えば、3次元フーリエ変換
4. 図36Cの信号まで処理ステップ1712
5. 信号としてパワースペクトルを生成し、図36Dの信号としてパワースペクトルを生成
6. この信号に対する1つの積分値を生成する。あるいは、図36Dの信号として積分値を生成
7. 再度、図36Dの信号として積分値を生成
8. 図36Dの信号として、1つのまたは2つのまたは3つの「ピーク」を生成
9. スケールを、図36Dの信号としてスケールを生成
10. 標準的なスケールのスケール値に一致する標準化パワースペクトルを生成
11. スケールにおける標準化パワースペクトルを生成
12. スケールにおける標準化パワースペクトルを生成
13. ここで実行した処理およびスケール
14. 標準化パワースペクトルを生成する。正確なスケールオフセットを生成
15. 何らかの「補正」を行い、図36Dのスケール、オフセットを正確に決定

【図38】



【図39】

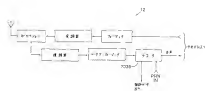


(1 1 1)

特開2005-51793(P2005-51793A)

【図40】

【図41A】



+	+
+	+

【図41B】

+	+
+	+

- 【手続補正書】
【提出日】平成16年12月21日(2004.12.21)
【手続補正1】
【補正対象書類名】明細書
【補正対象項目名】0499
【補正方法】変更
【補正の内容】
【0499】
【図1】2つの軌において分離された1次元デジタル信号の簡単な古典的な線図である。
【図2】“縦線”の検証信号を他の信号上に埋め込む処理の、ステップの詳細な記述による全体的な概観である。
【図3】オリジナルの疑わしいコピーをどのように検証するかについての漸次の説明である。
【図4】本発明の他の実施例による検証情報によってフィルムを前露光する装置の線図である。
【図5】本発明の“ブラックボックス”実施例の図表である。
【図6】図5の実施例のブロック図である。
【図7】異なるコードワードを有する同じノイズデータを有する入力データの連続する組を符号化するのに適合した図6の実施例の変形例を示す。
【図8】特有のコード番号を有するビデオテープ製造の各々のフレームを符号化するのに適合した図6の実施例の変形例を示す。
【図9a】本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。
【図9b】本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。
【図9c】本発明のある実施例において使用することができる製造標準ノイズ秒の表示である。
【図10】標準ノイズコードの検出において使用される集積回路を示す。
【図11】図10の実施例において使用することができる標準ノイズコードを検出する処理の流れを示す。
【図12】本発明の他の実施例による複数の検出器を使用する実施例である。
【図13】疑似ランダムノイズフレームを画像から発生する実施形態を示す。
【図14】信号の統計を復号化の補助においてどのように使用できるかを示す。
【図15】どのように署名信号を使用し、予測される歪み(例えば、MPEG)の観点におけるその歪みを増すかを示す。
【図16】ファイルについての情報をヘッダおよびファイル自体において評述する実施形態を示す。
【図17】ファイルについての情報をヘッダおよびファイル自体において評述する実施形態を示す。
【図18】回転対象パターンを使用する実施形態に関する詳細を示す。
【図19】回転対象パターンを使用する実施形態に関する詳細を示す。
【図20】回転対象パターンを使用する実施形態に関する詳細を示す。
【図21a】直線よりも“パシブ”の符号化を示す。
【図21b】直線よりも“パシブ”の符号化を示す。
【図22】セキュリティカードの模様を詳細に示す。
【図23】セキュリティカードの模様を詳細に示す。
【図24】セキュリティカードの模様を詳細に示す。
【図25】セキュリティカードの模様を詳細に示す。
【図26】セキュリティカードの模様を詳細に示す。

【図27】固有ノイズを有するデータオブジェクトに埋め込まれた情報を使用するネットワークリンク方法を説明する図である。

【図27A】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。

【図27B】代表的なウェブページと、自己抽出オブジェクトへのそのカプセル化におけるステップとを示す。

【図28】写真鑑別文書またはセキュリティカードの図である。

【図29】サブミナルデジタルクラティキュールを実現することができる2つの実施形態を示す。

【図29A】図29の実施形態における変形例を示す。

【図30】サブリミナルデジタルグラティキュールを実現することができる2つの実施形態を示す。

【図31A】 2つの傾斜軸に沿った空間周波数の位相を示す。

【図31B】2つの傾斜軸に沿った空間周波数の位相を示す。

【図32A】第1、第2および第3同心リングに沿った空間周波数の位相を示す。

【図32B】第1、第2および第3同心リングに沿った空間周波数の位相を示す。

【図B2C】第1、第2および第3同心リンクに沿った空間周波数の位相を示す。

【図33A】傾斜軸を使用するサブリミナルグラディキュールに対する登録プロセスにおけるステップを示す。

【図33B】傾斜靴を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。

【図33C】傾斜靴を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。

【図33D】傾斜鞋を使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。

【図B3E】傾斜靴を使用するサブリミナルグラディキュールに対する登録プロセスにおけるステップを示す。

【図34A】同心リングを使用するサブリミナルグラディキュールに対する登録プロセスにおけるステップを示す。

【図34B】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。

【図34C】同心リングを使用するサブリミナルグラティキュールに対する登録プロセスにおけるステップを示す。

【図34D】同心リングを使用するサブリミナルグラディキュールに対する登録プロセスにおけるステップを示す。

【図34E】同心リングを使用するサブリミナルグラディキュールに対する登録プロセスにおけるステップを示す。

【図35A】傾斜靴を使用するサブリミナルグラディキュールに対する他のステップを示す

【図35B】傾斜軸を使用するサブリミナルグラティキュールに対する他のステップを示す

【図35C】傾斜靴を使用するサブリミナルグラティキュールに対する他のステップを示す

【図36A】 2D FFTを必要としない他の登録プロセスを示す。

【図36B】 2D FFTを必要としない他の登録プロセスを示す。

【図36C】 2D FFTを必要としない他の登録プロセスを示す。

【図36D】2D FFTを必要としない他の登録プロセスを示す。

【図37】サブリミナルグラディキュールに対する登録プロセスを要約するフローチャートである。

【図38】好例の無線電話システムの主な部品を示すブロック図である。

【図39】図38のシステムの電話において使用することができる符号のステガノグラフィ的エンコードのブロック図である。

【図40】図1のセルサイトにおいて使用することができる符号のステガノグラフィ的データのブロック図である。

【図41A】符号化の一形態において使用する符号のビットセルを示す。

【図41B】符号化の一形態において使用する符号のビットセルを示す。

- (31)優先権主張番号 08/635,531
(32)優先日 平成8年4月25日(1996.4.25)
(33)優先権主張国 米国(US)

(特許庁注：以下のものは登録商標)

1. フロッピー
2. J A V A
3. ペンティアム